IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA v. WILLIAM BARONI, et. al, Defendants.	No. 15-cr-00193-SDW

DECLARATION OF ALEXANDER H. SOUTHWELL IN SUPPORT OF MOTION OF NONPARTY GIBSON, DUNN & CRUTCHER LLP TO QUASH SUBPOENA *DUCES TECUM*

Alexander H. Southwell, pursuant to 28 U.S.C. § 1746, hereby declares:

1. I am a partner at Gibson, Dunn & Crutcher LLP ("GDC"), and represent the Office of the Governor of New Jersey (the "OGNJ"). A request for my admission to the Court *pro hac vice*, as counsel for Nonparty GDC in the above-entitled case, is pending. Prior to joining GDC, I served as an Assistant United States Attorney in the United States Attorney's Office for the Southern District of New York. I received a Bachelor of Arts degree from Princeton University in 1993, and a Juris Doctor from New York University in 1997. I am also an Adjunct Professor of Law at Fordham University School of Law.

2. Attached hereto as Exhibit **A** is a true and correct copy of the letter from Randy M. Mastro to the Honorable Susan J. Wigenton, U.S. District Judge, dated June 8, 2015.

3. Attached hereto as Exhibit **B** is a true and correct copy of the letter from Randy M. Mastro to the Honorable Susan J. Wigenton, U.S. District Judge, dated June 10, 2015.

4. Attached hereto as Exhibit **C** is a true and correct copy of the following press release: Office of the Governor of N.J., Internal Review Team Puts Forward Comprehensive and

Exhaustive Report (Mar. 27, 2014), http://nj.gov/governor/news/news/552014/pdf/20140327a.pdf.

5. Attached hereto as Exhibit **D** is a true and correct copy of the following press release: Office of the Governor of N.J., Christie Administration Takes Steps to Conduct Internal Review and Further Cooperate with U.S. Attorney Inquiry (Jan. 16, 2014), http://www.state.nj.us/governor/news/news/552013/approved/20140116a.html.

6. Attached hereto as Exhibit **E** is a true and correct copy of the following article: Mark J. Magyar, *Much Ado about Nothing: No Tapes, Transcripts of Mastro Interviews,* NJ Spotlight (Apr. 9, 2014), http://www.njspotlight.com/stories/14/04/09/much-ado-about-nothing-no-tapes-transcripts-of-mastro-interviews/?p=all.

7. Attached hereto as Exhibit **F** is a true and correct copy of the following publication: *The Sedona Principles, Second Edition: Best Practices Recommendations and Principles for Addressing Electronic Document Production*, Introduction & cmt. 12 (Sedona Conference Working Group Series 2007).

8. Attached hereto as Exhibit **G** is a true and correct copy of this Court's guidelines for editing metadata: U.S. District Court for the District of New Jersey, *Guidelines for Editing Metadata*, available at http://www.njd.uscourts.gov/sites/njd/files/EditMetaDataGuidePublic.pdf

9. Attached hereto as Exhibit **H** is a true and correct copy of the following article: David Hricik, *I Can Tell When You're Telling Lies: Ethics and Embedded Confidential Information*, 30 J. Legal Prof. 79 (2006).

10. Attached hereto as Exhibit **I** is a true and correct copy of the following article: David Hricik & Chase Edward Scott, *Metadata: The Ghosts Haunting e-Documents*, 26 Computer & Internet Lawyer 23 (2009).

11. OGNJ retained GDC as outside counsel in January 2014 to undertake an internal investigation of conduct stemming from the realignment of lanes at the George Washington Bridge. In the process of undertaking this investigation, GDC was also asked by the OGNJ to investigate separate allegations in January 2014 by Hoboken Mayor Dawn Zimmer regarding the allocation of disaster relief aid following Superstorm Sandy.

12. During the course of the investigation, GDC interviewed multiple individuals. In all, GDC attorneys prepared 75 memoranda summarizing the witness interviews. GDC made these memoranda available to the U.S. Attorney's Office, the New Jersey Legislature's Select Committee on Investigation, and the public.

13. As GDC has explained in correspondence with the District Court, "[u]nder our protocol and practice for this investigation, witness interviews were summarized electronically by one attorney while the interviews were being conducted and then edited electronically into a single, final version. Those final interview memoranda were then printed and ultimately released publicly." Exhibit **A**, at 5.

14. As further explained to the Court: "We produced interview memoranda that we created, finalized and then released publicly." Exhibit **B**, at 1.

15. GDC personnel prepared the interview memoranda using the Microsoft Word program, and released them in PDF (Adobe Acrobat) format, leading to the recording of metadata associated with common operation of those computer programs. The metadata associated with the interview memoranda does not contain the contents of any versions of the interview memoranda.

16. On August 21, 2015, I caused to be served on Defendants, through counsel, the Objections and Responses of Nonparty Gibson, Dunn & Crutcher LLP to Order on Defendants'

Application For Subpoena *Duces Tecum*, a true and correct copy of which is attached hereto as Exhibit **J.** Those Objections and Responses make clear that no documents exist responsive to Item 1 of the subpoena *duces tecum* issued on July 10, 2015, on the application of Defendants, other than the 75 interview memoranda produced.

I hereby declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge. Executed on August 21, 2015.

Alexander H. Southwell

Exhibit A

GIBSON DUNN

Gibson, Dunn & Crutcher LLP

200 Park Avenue
New York, NY 10166-0193
Tel 212.351.4000
www.gibsondunn.com

June 8, 2015

The Honorable Susan D. Wigenton
United States District Judge
District of New Jersey
M.L. King Jr. Federal Building & Courthouse
50 Walnut Street
Newark, New Jersey 07102

Re: **United States v. Baroni, et al., 15 Cr. 193 (SDW)**

Dear Judge Wigenton:

We respectfully write as counsel to the Office of the Governor of New Jersey ("OGNJ") in response to Mr. Critchley's May 27 letter application ("Critchley Letter") (Doc. 16), made on behalf of the defendants in this criminal case, asking this Court to take the extraordinary step of issuing a Rule 17(c) subpoena to our law firm, Gibson Dunn & Crutcher, LLP ("Gibson Dunn"), concerning the internal investigation it conducted for the OGNJ. Mr. Critchley claims he wants to subpoena "[a]ny and all handwritten or typed notes, stenographic transcripts and audio and/or video recordings of witness interviews conducted by Gibson Dunn" during its investigation. Yet it has been a matter of public record since the spring of last year when we issued our report summarizing the findings of our investigation that we did not transcribe or record our interviews. And Mr. Critchley now acknowledges in his letter to the Court that he has all of our extensive interview memoranda—which he calls "summaries"—and that the U.S. Attorney's Office ("USAO") already told him that "they had asked Gibson Dunn for copies of the rough or draft notes from which the interview summaries were prepared and were told that none existed." Critchley Letter at 3-4. In short, Mr. Critchley has no good faith basis for seeking this subpoena, as he already knows the documents he seeks do not exist. We therefore respectfully request that the Court summarily reject Defendants' application.

We note at the outset that neither Mr. Critchley nor anyone else representing the Defendants contacted us before requesting this subpoena focused on transcripts and notes of Gibson Dunn's interviews during the internal investigation conducted on behalf of the OGNJ. Had they, we would have confirmed to them that no such documents ever existed. Specifically, Defendants' proposed subpoena seeks the production of "any and all handwritten or typed notes, stenographic transcripts and audio and/or video recordings of witness interviews conducted by Gibson Dunn during its representation of the Office of the

Governor of New Jersey from on or about January 16, 2014 to the present," as well as "any and all metadata and document properties for all typed notes and interview summaries created" during those interviews. Critchley Letter, Proposed Order (Doc. 16-1). Finally, Mr. Critchley requests explanations for any destroyed information without any legal or factual basis for such an extraordinary request. *Id.*

As this Court is well aware, Rule 17(c) has a specific and narrow purpose—it "is designed as an aid [in criminal cases] for obtaining [at the pretrial stage] relevant evidentiary material . . . admissible as evidence" at trial by the moving party. *United States v. Cuthbertson*, 630 F.2d 139, 144 (3d Cir. 1980) ("*Cuthbertson I*"). It is not meant to be used as "a means of discovery," or otherwise supplement Rule 16. *Id.*; *see also United States v. Nixon*, 418 U.S. 683, 698 (1974) (same). Rule 17(c) pretrial subpoenas must "constitute[] a good faith effort to obtain identified evidence," not "a general 'fishing expedition' that attempts to use the rule as a discovery device." *Id.* And such subpoenas must not be "unreasonable or oppressive." Fed. R. Crim. P. 17(c)(2). Accordingly, in order to establish that a subpoena is not unreasonable or oppressive under Rule 17(c)(2), a party seeking production "must clear three hurdles: (1) relevancy; (2) admissibility; (3) specificity." *United States v. Nixon*, 418 U.S. at 700; *see also United States v. Eisenhart*, 43 Fed. Appx. 500, 505 (3d Cir. 2002) (noting the *Nixon* factors). A party seeking production must show that "the application is made in good faith and is not intended as a general 'fishing expedition.'" *Cuthbertson I*, 630 F.2d at 145 (quoting *Nixon*, 418 U.S. at 699-700). "Courts must be careful that [R]ule 17(c) is not turned into a broad discovery device, thereby undercutting the strict limitation of discovery in criminal cases found in Fed. R. Crim. P. 16." *Cuthbertson I*, 630 F.2d at 146. The Third Circuit views "an impermissible discovery motive" as "an end run around *Nixon*" that is not to be tolerated. *United States v. Amirnazmi*, 645 F.3d 564, 595 (3d Cir. 2011). The Third Circuit has also warned against the "failure to discriminate between potential exculpatory material in the possession of the prosecution, generally available under the teachings of *Brady v. Maryland*, and exculpatory evidence in the possession of third parties. Only the latter is retrievable under a rule 17(c) subpoena; naked exculpatory material held by third parties that does not rise to the dignity of admissible evidence simply is not within the rule." *United States v. Cuthbertson*, 651 F.2d 189, 195 (3d Cir. 1981) ("*Cuthbertson II*").

Courts apply the *Nixon* factors strictly. For example, the Third Circuit has held that Rule 17(c) requires "more . . . to sustain a subpoena than the defendant's subjective belief (*i.e.*, hope) that he or she may find something useful by casting a subpoena upon the waters," *see Eisenhart*, 43 Fed. Appx. at 505, and courts in this Circuit have quashed subpoenas under Rule 17(c) because their requests were "speculative and extremely broad," without any "actual knowledge" by the moving party of the existence of the requested information, *see, e.g.*, *United States v. Tillman*, No. CRIM. 08-254, 2009 WL 3401721, at *1 (W.D. Pa. Oct.

20, 2009) (quashing Rule 17(c) subpoenas seeking, among other things, "all telephone calls made by [a government witness] while [in] prison" in part because the "requests [were] speculative and extremely broad," and the moving party "had no actual knowledge regarding whether the [prison] ha[d] any recorded . . . conversations of [the government witness]"). Indeed, when faced with a subpoena that is "not reasonably targeted toward the receipt of material admissible evidence," and whose requests are "speculative" and otherwise broad, it is necessary for the court to refuse to issue, to quash or, at a minimum, to narrow the scope of the subpoena. *Id.* Similarly, a Rule 17(c) subpoena is improper under the *Nixon* factors if it seeks documents that are not admissible at trial under the Federal Rules of Evidence or if it seeks pretrial materials simply for impeachment purposes. *See Tillman*, 2009 WL 3401721, at *1. Courts must also consider applicable privileges in determining whether a Rule 17(c) subpoena is overbroad or oppressive. *See, e.g.*, *United States v. Friedman*, 854 F.2d 535, 571 (2d Cir. 1988) (affirming quashing of subpoena for psychiatric records).

Defendants' proposed requests fall far short of Rule 17(c)'s good-faith requirement—the requests are extremely broad and speculative, and are not reasonably targeted at admissible evidence. Defendants seek a broad swath of attorney notes and information, yet offer no specificity by subject and instead cast an impermissibly broad net through their proposed requests. Indeed, the over-reaching character of Defendants' proposed subpoena is confirmed by the fact that a bulk of the interview memoranda that Defendants seek relate to the Hoboken allegations addressed in the Gibson Dunn Report, which are completely irrelevant to the criminal charges against Defendants. With respect to Defendants' request for the metadata for all interview memoranda, Defendants purport to seek this data in order to "identify who created the summaries, who, if anyone, edited the summaries, and when." Critchley Letter at 12. But Defendants nowhere explain why this metadata is relevant or how it could reasonably yield admissible evidence. And they cannot do so—because file metadata only potentially shows information like the dates a file was created or accessed; it shows nothing about the substance of any edits. Further, metadata can be altered by actions that do not alter or even open for viewing the substance of the material in the file itself, such as simply moving a file into a new folder. Such information clearly is not the specific "admissible . . . evidence" required by Rule 17(c). *Cuthbertson II*, 651 F.2d at 192. Moreover, as Mr. Critchley goes to lengths to point out, the public interview memoranda themselves indicate the attorneys present for each interview, obviating any alleged need for metadata information. Finally, Mr. Critchley requests, without any legal or factual basis for such an extraordinary request, that the Court require us to explain what he claims is "destroyed" information. Critchley Letter at 11. As explained herein, there was no "destruction" of evidence here, and his rhetoric displays a fundamental misunderstanding of the process by which we summarized our interviews. The subpoena application should therefore be denied.[1]

Significantly, Defendants' own application belies the requested speculative subpoena because Mr. Critchley concedes that no interview transcripts, recordings, or notes memorializing our interviews exist. As Mr. Critchley notes in his own letter, the USAO made it clear to him that Gibson Dunn does not have any rough or draft notes of interviews. Critchley Letter at 4. Indeed, this information was publicly confirmed in April of last year, when New Jersey Assemblyman John Wisniewski, Chairman of the Select Committee on Investigation ("SCI"), announced that it was his understanding that there were no recordings or transcripts from the Gibson Dunn interviews. In other words, Mr. Critchley filed a 13-page application seeking imaginary materials that he admits to knowing do not exist.[2]

[1] This Court need not address doctrines of privilege here; OGNJ is not asserting privilege over the requested materials because such records do not exist. It nevertheless warrants mention that Defendants err in contending that privilege has been waived through an effort to invoke it "selective[ly]." Critchley Letter at 9. The extrajudicial disclosure of certain privileged material merely constitutes a "partial waiver," which, in the circumstances of this case, permitted the OGNJ to "disclose[] a portion of privileged communications" and still "to continue asserting the privilege as to the remaining portions of the same communications." *Westinghouse Elec. Corp. v. Repub. of Philippines*, 951 F.2d 1414, 1423 n.7 (3d Cir. 1991). "When a party discloses a portion of otherwise privileged materials while withholding the rest, the privilege is waived only as to those communications actually disclosed, unless a partial waiver would be unfair to the party's adversary." *Id.* at 1426 n.12 (citing *In re Von Bulow*, 828 F.2d 94 (2d Cir. 1987)); *see also id.* at 1430 ("partial . . . disclosure[]" analysis for attorney-client privilege "applies equally in the context of the work-product doctrine"); *Von Bulow*, 828 F.2d at 102 ("the extrajudicial disclosure of an attorney-client communication—one not subsequently used by the client in a judicial proceeding to his adversary's prejudice—does not waive the privilege as to the undisclosed portions of the communication.").

[2] Among his many misleading and irrelevant assertions, Mr. Critchley notes that two witnesses stated under oath that the interview memoranda were "incorrect in critical respects." Critchley Letter at 6. In fact, both witnesses specifically took issue only with a few phrases contained in our summaries of their interviews and Mr. Critchley points only to those two individuals' limited critique out of the 75 interview memoranda prepared by our firm. Gibson Dunn conducted all interviews with at least two lawyers present to enhance the accuracy of the memorandum preparation. Moreover, Mr. Critchley erroneously claims Gibson Dunn had as many as six attorneys participating in

Gibson Dunn has no recordings, transcripts, or notes memorializing our interviews, other than the interview memoranda summarizing Gibson Dunn's interviews. Under our protocol and practice for this investigation, witness interviews were summarized electronically by one attorney while the interviews were being conducted and then edited electronically into a single, final version. Those final interview memoranda were then printed and ultimately released publicly. Mr. Critchley is asking for interview recordings, transcripts, and notes that he knows do not exist. And to the extent he seeks metadata regarding our interview memoranda, that would yield only certain dates and times the documents were accessed in some way, not any interview contents or other substantive information that would be relevant or admissible in this case. In short, there is no good faith basis for issuance of a subpoena here.

While I appreciate that Mr. Critchley makes this application as a zealous advocate representing a defendant facing serious criminal charges, there are bounds to what we, as officers of the court, should allege, without basis. As counsel representing a public office and as a former federal prosecutor myself, I am representing to this Court, as we did to the U.S. Attorney's Office while it was conducting its investigation of this case, that we do not have any recordings, transcripts or notes of our interviews. So Mr. Critchley is now seeking records known not to exist—and making reckless, unfounded allegations in the process—in what appears to be an attempt to distract attention away from his client's misconduct, which was detailed in our report and then confirmed in two other separate investigations, including the one that led to these criminal charges. The fact is that we have no recordings, transcripts or notes of our interviews, only our already-released interview memoranda. Hence, it would serve no purpose to issue a subpoena here, because the documents sought do not exist.

Accordingly, we respectfully request that the Court put an immediate end to this misguided attempt to subpoena our law firm and deny Defendants' subpoena application now.

Respectfully,

Randy Mastro

one interview. This is untrue. Gibson Dunn interviewed certain witnesses multiple times, and different attorneys participated in those multiple interviews. Hence, each witness interview memorandum identified any attorney who participated in any portion of the multiple interviews of the witness.

cc (*via e-mail*):
Lee M. Cortes, Jr., Assistant U.S. Attorney
Vikas Khanna, Assistant U.S. Attorney
David W. Feder, Assistant U.S. Attorney
Michael Critchley, Esq.
Michael Baldassare, Esq.

Exhibit B

GIBSON DUNN

Gibson, Dunn & Crutcher LLP

200 Park Avenue
New York, NY 10166-0193
Tel 212.351.4000
www.gibsondunn.com

Randy M. Mastro
Direct: +1 212.351.3825
Fax: +1 212.351.5219
RMastro@gibsondunn.com

June 10, 2015

The Honorable Susan D. Wigenton
United States District Judge
District of New Jersey
M.L. King Jr. Federal Building & Courthouse
50 Walnut Street
Newark, New Jersey 07102

Re: **United States v. Baroni, et al., 15 Cr. 193 (SDW)**

Dear Judge Wigenton:

We respectfully write as counsel to the Office of the Governor of New Jersey ("OGNJ") to reply briefly to Mr. Critchley's letter of yesterday (Doc. 18) concerning Defendants' application for a Rule 17(c) subpoena directed at our law firm ("Gibson Dunn") for transcripts, recordings, or notes of the interviews we conducted during our investigation on behalf of the OGNJ. Mr. Critchley now claims that we "created" what he calls "electronic interview notes" but they "allegedly no longer exist." Doc. 18 at 2. Of course, because he acknowledges no such notes "exist," he is admitting the subpoena that he seeks would serve no purpose. Moreover, he mischaracterizes our process and misapprehends the facts. As I explained in my June 8 letter, we created an interview memorandum electronically as each interview was conducted, edited that electronic file to produce a " single, final version," and those "final interview memoranda were then printed and ultimately released publicly." In other words, it is a misnomer to describe our process as ever having involved the "creat[ion]" of "electronic interview notes" that we should have preserved. We produced interview memoranda that we created, finalized and then released publicly. And the limited metadata we have concerning these interview memoranda would yield no admissible evidence whatsoever, revealing only certain times each file was accessed, not any substance from the interviews themselves. Hence, we have nothing else responsive to this proposed subpoena, other than our already-released interview memoranda. In the face of our thorough explanation of this point, Mr. Critchley's repeated references to "electronic interview notes" that do not exist—and never did—can only be construed as a purposeful misreading of my June 8 letter.[1] As a result, his application must fail because he cannot meet the strict standard for issuance of a Rule 17(c) subpoena.

[1] In a contrived attempt to justify subpoenaing our law firm, Mr. Critchley also mischaracterizes our findings as supposedly deviating from the criminal charges his

Respectfully,

Randy Mastro/ls

Randy Mastro

cc (*via e-mail*):
Lee M. Cortes, Jr., Assistant U.S. Attorney
Vikas Khanna, Assistant U.S. Attorney
David W. Feder, Assistant U.S. Attorney
Michael Critchley, Esq.
Michael Baldassare, Esq.

client now faces. He claims that our investigation concluded the motive for this lane realignment was *not*, as the indictment charges, to retaliate against Fort Lee Mayor Sokolich for declining to endorse Governor Christie for re-election. Doc. 18 at 2-3. That is not so. In reality, we concluded in our report that "David Wildstein (then of the Port Authority) and Bridget Kelly (then one of the Deputy Chiefs of Staff in the Governor's Office) knowingly participated in this plan to realign toll lanes leading onto the George Washington Bridge at Fort Lee, at least in part, for some ulterior motive to target Mayor Sokolich." Report at 2. We then went on to explain that "there are persuasive reasons to believe that the lane realignment was, in fact, motivated to target Mayor Sokolich for some reason. The specific reason or reasons that Wildstein and Kelly wanted to target him—whether Sokolich's unwillingness to endorse or some other conduct that they found objectionable—is, however, more difficult to determine. . . . But this is a question we are unable to answer, even after a thorough investigation." Report at 106. Thus, there is no inconsistency between our findings and the pending criminal charges, with both finding ulterior motives to target Mayor Sokolich and the criminal investigation able to allege a specific motivation, presumably because of Mr. Wildstein's cooperation.

Exhibit C

Internal Review Team Puts Forward Comprehensive and Exhaustive Report

After More Than 70 Interviews And 250,000 Documents Reviewed Over Two Months, The Internal Review Team From Gibson Dunn Report Their Findings After Thorough Investigation

KEY TAKEAWAYS:

- Governor Christie did not know, and had no involvement in the decision to realign the lanes.
  - There is also no evidence that the Governor knew of the lane realignment while it was occurring.
- There is no evidence that any member of the Governor's staff, besides Bridget Kelly, was involved in the decision to realign the lanes or took any action to cover it up.
  - Speculation that there was a culture of retaliation within the Governor's Office is "unsubstantiated."
- David Wildstein and Bridget Kelly "knowingly participated in this plan … at least in part, for some ulterior motive to target Mayor Sokolich."
  - "The participants in this plan were not authorized by Governor Christie or anyone else in the Office of the Governor to realign or alter the George Washington Bridge Fort Lee access lanes."
  - Wildstein first raised the issue of toll lane access in Fort Lee in 2010, and "seemed to be driving the issue again in 2013."
  - Kelly attempted to conceal her actions following a "grilling" by Chief of Staff Kevin O'Dowd, by asking Christina Renna to delete her email replying "good" after being informed Mayor Sokolich was "extremely upset."
  - Some evidence shows that Kelly and Wildstein had "a focus and animus toward Sokolich not explicitly tied to his endorsement."
  - There is no evidence of anyone else having "knowingly participated in this plan to target Mayor Sokolich."
  - Bill Baroni and Bill Stepien knew of the idea to realign the lanes in advance, though not necessarily any ulterior motives.
- Five former federal prosecutors led the team which conducted a review spanning more than two months to produce the nearly 350 page report with more than 600 cited exhibits included in the final release.
  - More than 70 interviews were conducted including with Governor Christie, Lt. Governor Guadagno, and the entire senior staff of the Governor's Office and other relevant individuals.
  - 250,000 documents were reviewed "including the personal texts and emails of the Governor, the Lieutenant Governor, and their senior staffers."
  - A copy of the report was provided to the US Attorney's Office and the Legislative Select Committee.

THE GOVERNOR HAD NO PRIOR KNOWLEDGE OF LANE REALIGNMENT:

Governor Christie Did Not Know, And Had No Involvement In Decision To Realign The Lanes. "Our investigation found that Governor Christie did not know of the lane realignment beforehand and had no involvement in the decision to realign the lanes." (p. 10)

- **There Is Also No Evidence That The Governor Knew Of The Lane Realignment While It Was Occurring.** "Nor did we find any credible evidence that the Governor had knowledge of the lane realignment while it was occurring from September 9 to 13, 2013. … Our examination … found no evidence that the Governor had knowledge of the lane realignment during its implementation." (p. 127 – 128)
- **The Investigation "Uncovered Nothing Contradicting The Governor's Account."** "[I]n all the documents we reviewed (including the personal texts and emails of the Governor and his senior staff) and from all the witnesses we interviewed, we uncovered nothing contradicting the Governor's account." (p. 11)

The Review Confirms The Governor's Account From The January 8th Press Conference:

- **October 2013: Following The Publication Of The Foye Email By *The Wall Street Journal,* Governor Christie Asked Charlie McKenna To Look Into The Issue, Who Was Assured By Bill Baroni That It Was Part Of A Legitimate Traffic Study.** "After the publication of the October 1 *Wall Street Journal* article, at the Governor's direction, McKenna questioned Baroni, who assured McKenna that the lane realignment had been a legitimate Port Authority traffic study; McKenna communicated Baroni's assurances to the Governor." (p. 124)
- **December 12: Following Testimony By Port Authority Officials And As Rumors of Bridget Kelly's Involvement Emerged, "The Governor Became Concerned About What He Was Hearing And Demanded Straight Answers From His Senior Staff."** "Others also heard the Kelly email rumors and reported them back to the Governor's Office around that time. On December 9, 2013, Port Authority officials testified before the Assembly Committee that Wildstein was behind the lane realignment decision and told them 'not to worry' about notifying Foye or Fort Lee officials in advance. Foye also testified, saying he was not aware of any actual traffic study. The Governor became concerned about what he was hearing and demanded straight answers from his senior staff."(p. 8)
  - **Governor Christie Directly Asked Stepien "What, If Anything, He Knew," Stepien "Denied Having Any Involvement" Saying Wildstein Had "50 Crazy Ideas A Week."** "[G]overnor Christie asked Stepien what, if anything, he knew about the lane realignment. Stepien denied having any involvement in the lane realignment decision or its implementation. Rather, Stepien told the Governor that Wildstein would come to him with '50 crazy ideas a week …'" (p. 94)
  - **When Questioned By Chief Of Staff Kevin O'Dowd, Kelly "Unequivocally Denied Any Contemporaneous Knowledge."** "[O]'Dowd asked Kelly if she knew anything about the lane realignment before it went into effect. Kelly unequivocally denied any contemporaneous knowledge of the lane realignment. Kelly also asked O'Dowd why he was asking. O'Dowd responded that the Governor had directed him to talk to her. O'Dowd inquired further whether she had any text messages or emails on the subject, and Kelly responded that she did not think so. Nonetheless, O'Dowd directed Kelly to review her text messages and emails and check if she had any evidence on the question. O'Dowd further instructed Kelly that she should let him know right away if she found anything. O'Dowd then informed Governor Christie of Kelly's denial of any contemporaneous knowledge of the lane realignment." (p. 95)
- **December 13: Governor Christie Convened His Senior Staff And Demanded They Come Forward With Any Information They Had, Saying Of The Bridge Fiasco: "This Is A Mess, And Now I Have To Clean It Up."** "[O]n December 13, 2013, the Governor convened a special meeting of his senior staff and also invited Drewniak. He stood the entire time and raised his voice. He told them he was concerned they were all suffering from 'senioritis' following the election. … He mentioned a number of miscues but then focused on the George Washington Bridge lane realignment fiasco. He said words to the effect of: "This is a mess, and now I have to clean it up." He demanded to know from each of them in that room whether they had any prior knowledge or involvement with the lane realignment." (p. 9)

- - **After The Meeting, Kelly Was Directly Questioned A Second Time By O'Dowd And Continued To Deny Involvement.** "He told them to come forward with the truth that morning, to go tell O'Dowd or Charles McKenna, then the Governor's Chief Counsel. … But Kelly did not come forward. To the contrary, when questioned for a second time by O'Dowd that morning, Kelly continued to deny any involvement." (p. 9)

- **January 8, 2014: Governor Convened His Senior Staff And "Expressed Shock" At The New Revelations And Directed The Dismissal Of Kelly And Stepien.** "That afternoon, on January 8, 2014, the Governor called together his top aides and advisors at Drumthwacket. It was an emotional session, in which the Governor, welling up with tears, expressed shock at the revelations, directed Kelly's immediate firing for lying to him, and also decided to sever ties with Stepien." (p. 10)

WITH THE EXCEPTION OF BRIDGET KELLY, NO OTHER MEMBER OF THE GOVERNOR'S STAFF WAS INVOLVED:

There Is No Evidence That Any Member Of The Governor's Staff, Besides Bridget Kelly, Was Involved In The Decision To Realign The Lanes Or Took Any Action To Cover It Up. "We have not found any evidence of any other member of the Governor's staff, besides Bridget Kelly, being involved in the decision to realign these George Washington Bridge toll lanes at Fort Lee. And we have not found any evidence of any other member of the Governor's staff, besides Bridget Kelly, doing anything to cover up what happened here after the fact." (p. 11)

- **"Kelly Approved The Lane Realignment Plan, Stayed Involved Throughout, And Then Participated In A Cover Up"** "In sum, we find that Kelly approved the lane realignment plan, stayed involved throughout, and then participated in a cover up of it afterward. Mayor Sokolich also appears to have been targeted for some reason yet to be determined." (p. 115)

- **"[K]elly Deliberately Deceived Governor Christie And The Rest Of The Governor's Office Senior Staff …"** (p. 115)

There Is No Evidence Of Any Cover-Up Within The Governor's Office. "To the contrary, when, by early December 2013, allegations of Kelly's involvement surfaced – however vague and speculative those allegations were at the time – the Governor personally had further inquiry made and demanded full disclosure by his senior staff." (p. 133)

The Investigation Also Found Speculation That The Governor Created A Culture Of Retaliation To Be "Unsubstantiated." "Following the lane realignment, several New Jersey legislators have claimed that Governor Christie created a 'culture' of 'abuse of power' condoning retaliation against political adversaries. … In response to these allegations, we have endeavored to determine whether or not Governor Christie condoned, encouraged, or directed those working in his Office to engage in partisan retaliation. Our investigation found such speculation to be unsubstantiated." (p. 134)

BRIDGET KELLY AND DAVID WILDSTEIN WERE TARGETING MAYOR SOKOLICH:

David Wildstein And Bridget Kelly "Knowingly Participated In This Plan … At Least In Part, For Some Ulterior Motive To Target Mayor Sokolich." "Our investigation found that David Wildstein (then of the Port Authority) and Bridget Kelly (then one of the Deputy Chiefs of Staff in the Governor's Office) knowingly participated in this plan to realign toll lanes leading onto the George Washington Bridge at Fort Lee, at least in part, for some ulterior motive to target Mayor Sokolich." (p. 2)

- **Wildstein First Raised The Issue Of Toll Lane Access In Fort Lee In 2010, And "Seemed To Be Driving The Issue Again In 2013."** "Indeed, Wildstein himself first raised the issue in late 2010. For some reason yet to be determined, Wildstein seemed to be driving this issue again in 2013. It was Wildstein's 'idea,' like so many other 'crazy' ones he'd had before that never got off the ground." (p. 3)

  - **Wildstein "Originated, Effectuated, And Oversaw" The Lane Realignments, And Even Admitted They Were His "Idea."** "The evidence establishes that David Wildstein originated, effectuated, and oversaw the September 2013 George Washington Bridge lane realignment operation. … Indeed, although Wildstein refused to cooperate with our investigation and has asserted his Fifth Amendment rights, he admitted to McKenna and others that the lane realignment was his 'idea.' Our review of the evidence is consistent with the Port Authority's conclusion and Wildstein's admissions." (p. 107-108)

- **Some Evidence Shows That Kelly And Wildstein Had "A Focus And Animus Toward Sokolich Not Explicitly Tied To His Endorsement."** "Indeed, it seems unlikely that political retaliation for Sokolich's unwillingness to endorse could have been the true objective of the lane realignment. After all, Mayor Sokolich made that decision known five months earlier – without any apparent effect on his working relationship with the Governor's Office thereafter. … Other evidence also reflects a focus and animus toward Sokolich at the time that was not explicitly tied to his decision not to endorse the Governor." (p. 112)
    - **Kelly Was "Irate" When Informed That A Staffer Had Met With Mayor Sokolich On August 16.** "We found no evidence up until that point in time of any hostility toward Mayor Sokolich. But when Kelly learned that one of her staffers … met with Mayor Sokolich a few days later on August 16, 2013, she lashed out about it in a series of emails, saying 'I am on fire,' 'I am irate,' '[W]hy did he think it was ok to meet with Sokolich?,' and 'He should not have met with Fort Lee without approval. I am really upset with him.'" (p. 4)

"The participants in this plan were not authorized by Governor Christie or anyone else in the Office of the Governor to realign or alter the George Washington Bridge Fort Lee access lanes." (p. 105)

- **There Is No Evidence Of Anyone Else Having "Knowingly Participated In This Plan To Target Mayor Sokolich."** "As to whether anyone else may have knowingly participated in this plan to target Mayor Sokolich, our investigation has not found any evidence of anyone else's involvement." (p. 2)

Bill Baroni And Bill Stepien Knew Of The Idea To Realign The Lanes In Advance, Though Not Necessarily Ulterior Motives. "Our investigation also found that Bill Stepien (then the Governor's campaign manager) and Bill Baroni (then the Deputy Executive Director of the Port Authority) knew of this idea in advance, but we found no evidence that they knew of the ulterior motives here, besides the claimed purpose of conducting a traffic study." (p. 2)

<u>KELLY ATTEMPTED TO CONCEAL HER ACTIONS BY REQUESTING EMAIL DELETED:</u>

Following The "Grilling" By O'Dowd On December 12, Kelly Asked Christina Renna To Delete Her Email Replying "Good" After Being Informed That Mayor Sokolich Was "Extremely Upset." "On December 12, 2013, he had further inquiries made of Kelly and Stepien. Both denied any involvement in the decision to close these lanes. … [K]elly was nevertheless panicked by what she considered to be O'Dowd's 'grilling.' She called her staffer, Christina Renna, that same night to make a desperate request: delete the email that Kelly sent Renna on September 12, 2013, where Kelly, upon learning Mayor Sokolich was 'extremely upset,' responded: 'Good.'" (p. 8)

- **"Despite Kelly's Attempt To Cover Her Tracks, Renna Preserved A Copy Of That Email."** (p. 8)

The Morning After Being Fired, Kelly Sent A Text To Renna "Admitting Her Transgression: 'I'm Sorry To Tarnish IGA.'" "The next morning, on January 9, 2014, the Governor held a press conference for nearly two hours in which he acknowledged this breach by someone close to him, took responsibility for it happening on his watch, and answered the press's questions. That same morning, Kelly texted her then-former staffer, Renna, admitting her transgression: 'I'm sorry to tarnish IGA.'" (p. 10)

<u>GIBSON DUNN RECOMMENDATIONS TO PREVENT SIMILAR INCIDENTS:</u>

The Office Of The Governor:

- **Restrict The Use Of Personal Email Accounts For Official State Business:** Employees within the Governor's Office should no longer be allowed to use personal email accounts to conduct state business absent extraordinary circumstances.

- **Eliminate The Office Of Intergovernmental Affairs:** In light of the aberrational behavior that occurred here and to eliminate any misconceptions going forward, IGA should be disbanded and its functions reorganized within a new and expanded Governor's Office of Constituent and Legislative Services.

- **Institute An Ombudsperson Within The Governor's Office:** A senior statesperson "of unquestioned integrity and independence," should be appointed ombudsperson within the Governor's office who reports directly to the Governor. The role would be to serve as a sounding board for complaints and ensuring that appropriate response to issues.

- **Appoint A Chief Ethics Officer:** To ensure what happened here will not be repeated moving forward, the Governor should appoint a Chief Ethics Officer. This newly created position will be dedicated to addressing ethics issues and conflicts as they arise while overseeing training to ensure Governor's office staff are aware of their obligations.

The Port Authority Of New York And New Jersey:

- **Appoint Bi-State Commission To Review Restructuring The Port Authority:** In conjunction with New York, New Jersey should move to form a bi-state commission to formulate a reorganization of the Port Authority. As a priority, the commission should consider a potential fundamental restructuring of the PA's organization and the appointment process for PA commissioners and senior executives.

- **Propose Legislative Reforms To Promote Transparency:** The Governor's office should work with legislative leaders and their New York counterparts to craft new or modified reform proposals to bring enhanced transparency and accountability to across the region's public authorities.

Exhibit D

Christie Administration Takes Steps To Conduct Internal Review And Further Cooperate With U.S. Attorney Inquiry

Thursday, January 16, 2014 Tags: Other

Former AUSA for the Southern District of New York To Lead Gibson, Dunn & Crutcher LLP Team

Trenton, NJ – Today, the Christie Administration announced the retention of Gibson, Dunn & Crutcher LLP to assist with the internal review announced by Governor Christie last week and to further cooperate with the U.S. Attorney inquiry. As part of the review process, Gibson, Dunn & Crutcher LLP will review best practices for office operations and information flow, and assist with document retention and production.

"Governor Christie made clear last week that he will conduct an internal review to uncover the facts surrounding the lane closures in Fort Lee. His Administration is fully cooperating with the U.S. Attorney inquiry and other appropriate inquiries and requests for information. To assist in conducting that internal review and furthering that cooperation, the Christie Administration is announcing today that Gibson, Dunn & Crutcher LLP has been retained as outside counsel. Their presence will bring an outside, third-party perspective to the situation, and they will be a valuable asset as we move forward. This Administration is committed to ensuring that what happened here never happens again. That's what the people of New Jersey deserve."

Heading up the Gibson, Dunn & Crutcher LLP team is former federal prosecutor Randy Mastro. Mastro is a former Assistant United States Attorney for the Southern District of New York, where he specialized in organized crime cases and spearheaded the federal government's landmark racketeering suit that compelled the International Brotherhood of Teamsters to hold democratic elections and to undergo court supervision. Mastro also served as former Deputy Mayor of New York City.

# # #

Press Contact:
Michael Drewniak
Colin Reed
609-777-2600

Stay Connected
with Social Media

Stay Connected
with Email Alerts

Submit Que

LIKE THIS PAGE? SHARE IT WITH YOUR FRIENDS.

SHARE

OPRA | Open Public Records Act

Contact Us | Privacy Notice | Legal Statement & Disclaimers | Accessibility Statement |

Statewide: NJ Home | Services A to Z | Departments/Agencies | FAQs
Office of the Governor: Home | Newsroom | Media | Administration | NJ's Priorities | Contact Us

Office of the Governor
PO Box 001
Trenton, NJ 08625
609-292-6000

Exhibit E

NJ SPOTLIGHT
NEWS, ISSUES AND INSIGHT FOR NEW JERSEY

MUCH ADO ABOUT NOTHING: NO TAPES, TRANSCRIPTS OF MASTRO INTERVIEWS

MARK J. MAGYAR | APRIL 9, 2014

Assemblyman John Wisniewski (D-Middlesex), cochairman of the Joint Select Committee on Investigation, and Senate Majority Leader Loretta Weinberg (D-Bergen).

Legislative investigators may be headed toward a legal showdown with Gov. Chris Christie and his team of lawyers to obtain the **documentary evidence that was used to clear the governor** and his top aides of wrongdoing in Bridgegate and other Port Authority-related scandals.

But the "evidence" may be of little value.

Assemblyman John Wisniewski (D-Middlesex), cochairman of the Joint Select Committee on Investigation, said yesterday it is his understanding that Randy Mastro and his Gibson Dunn & Crutcher firm not only failed to conduct the 70 interviews under oath, but also failed to videotape, audiotape, or have a stenographer make transcripts of any of the interviews.

"If this was supposed to be a transparent 360-degree examination of what happened, the lack of any hard evidence of what people said and how they responded to questions means that this report is based upon nothing more than the (Mastro team's) mental impressions of what people said," Wisniewski noted. "That's the classic definition of hearsay," he said, dismissing the conclusions of the $1 million **taxpayer-funded study**.

Nevertheless, Wisniewski and Senate Majority Leader Loretta Weinberg (D-Bergen) said the committee wants whatever interview memos or other documentary evidence that does exist. They said the panel would give the governor's office and Mastro's firm only until Friday to provide the materials voluntarily before issuing a subpoena.

Wisniewski also announced that the governor's office, Christie's reelection campaign and former **Port Authority Chairman David Samson** are the only three entities and individuals who have yet to fully comply with the wave of 28 subpoenas issued by the panel in late January.

Wisniewski said he did not believe the panel has received records of Christie's cellphone, emails, and text messages, and added that the committee has received little from Samson, who refused to be interviewed by the Mastro committee and whose alleged conflicts of interest at the Port Authority are the subject of a probe by the U.S. Attorney in the Southern District of Manhattan and of complaints to the state Ethics Commission.

Weinberg and Wisniewski announced the prospective subpoena and the absence of any tapes or transcripts of the Mastro team interviews in a **press conference after a meeting of the investigative committee** that followed four days of explosive developments in the Bridgegate scandal:

- U.S. Attorney for New Jersey Paul Fishman is presenting witnesses to a 23-member **federal grand jury** empaneled for 18 months that is apparently investigating both the George Washington Bridge lane closures and **Hoboken Mayor Dawn Zimmer's allegation** that the Christie administration threatened to withhold Sandy aid if she did not support a high-rise development project represented by Samson. Christie press secretary Michael Drewniak testified last Friday.

- David Wildstein, Christie's political lieutenant at the Port Authority who directed the George Washington Bridge lane closures and claims to have told Christie about them while they were happening, met with Fishman's investigators for three days last week, a reporter who used to cover Christie's U.S. Attorney's Office reported on the **Main Justice website**. It is the latest evidence that Wildstein may be close to the immunity deal he has been seeking.
- The Main Justice story also reported that Charles McKenna, Christie's chief counsel, met secretly with Fishman's office in mid-January. This was just a few days after the release of Deputy Chief of Staff Bridget Kelly's infamous "time for some traffic problems in Fort Lee" email first tied the scandal directly into the governor's office. McKenna, who now heads the Schools Development Authority, can provide inside information on the internal response of the Christie administration to the Bridgegate scandal: It was McKenna who questioned Port Authority Deputy Executive Director Bill Baroni, Wildstein's boss, at Christie's direction after the Wall Street Journal published Port Authority Executive Director Patrick Foye's email alleging that the lane closures may have broken federal and state law.
- Finally, Senate President Stephen Sweeney (D-Gloucester) on Monday undercut the legislative investigation when he told the Star-Ledger editorial board that the committee should suspend its Bridgegate probe if a federal judge declined to order the cooperation of Bridget Kelly and Bill Stepien, Christie's former deputy chief of staff and campaign manager, who have invoked their Fifth Amendment rights in the Bridgegate case. While Sweeney recanted later in the day after Wisniewski protested, his initial statement cast doubt on his commitment to the ongoing probe.

Weinberg yesterday shrugged off Sweeney's assertion as a "miscommunication" or an "inartful" response to a question, and both she and Wisniewski expressed confidence that the powerful Senate president was fully supportive of the continuation of their probe.

Nevertheless, Sweeney's statement came as Republican leaders, including GOP members of the Select Committee on Investigation, have been urging the committee to focus on enacting legislation to reform the Port Authority and to leave investigation of the machinations of the Bridgegate scandal to the U.S. Attorney's Office and the grand jury.

Assemblywoman Holly Schepisi (R-Bergen) made that case on MSNBC over the weekend, and Assemblywoman Amy Handlin (R-Monmouth) took the lead yesterday in urging the Democratic majority on the committee to pass a 16-bill package of legislation that she and other GOP lawmakers have sponsored, some of which are similar to those Wisniewski and Weinberg have sponsored in the past.

"What is stopping us from moving forward on our bills today?" Handlin asked, holding up a three-inch stack of legislation for the bank of 12 TV cameras covering the hearing.

Handlin said she didn't understand Wisniewski's insistence on completing the committee's investigation of the causes and coverup of the George Washington Bridge lane closures before enacting reform legislation.

"I don't understand the notion of 'no culprit, no reform,'" she said. "If I'm walking down the street and see a stabbing victim, don't you think I should stop the bleeding and not wait for the police to catch the culprit first?"

"We don't know who the culprit is, who closed the lanes or how far this goes," Wisniewski shot back, noting that Christie vetoed legislation two years ago sponsored by Weinberg that would have implemented reform measures similar to some of those Handlin was pushing. "Maybe you're content with the way the governor's office treats the Port Authority as just another desk in the governor's office, but I'm not."

Wisniewski opened the committee hearing with an impassioned defense of the need for the investigative committee to continue its work -- a defense that seemed to be aimed equally at Sweeney's statement Monday and at the growing barrage of Republican criticism. He noted that the committee's job is "to understand how these politically motivated lane closures could have happened and to develop a legislative response.

“To suggest that the Gibson Dunn report provides all of the information that we need to know is to frankly deliberately ignore its critical deficiencies, which are numerous,” Wisniewski said. “To suggest that the U.S. Attorney’s work will suffice is to deliberately ignore the strictly criminal focus of the U.S. Attorney’s probe and the limited public disclosure that comes along with it.”

He reminded the panel that “our investigation had its genesis in its examination of the Port Authority and its deficiencies,” adding that it was the Assembly Transportation Committee’s original “painstaking work” that led the Bridgegate investigation to the governor’s office.

Wisniewski got into a shouting match at the end of the short public session with Sen. Kevin O’Toole (R-Essex), Christie’s closest ally on the investigative committee, and made it clear that he was exasperated with Mastro’s firm for holding back thousands of pages of documents subpoenaed by the committee until the evening before the release of the report.

Kevin Roberts, the governor’s press spokesman, did not respond to an emailed question asking whether Wisniewski was correct that no tapes or transcripts existed from the 70 interviews, but that appears to be the case based on Mastro’s statement, which referred only to interview memos.

"We reached out to counsel for the committee over a week ago to discuss sharing voluntarily the interview memoranda regarding the lane realignment upon which our report was partially based,” Mastro said in a statement forwarded by Roberts. “In light of the committee's statements this afternoon, we will look forward to continuing that cooperative dialogue.”

Wisniewski acknowledged that the committee’s legal team has had discussions with Mastro, but noted that it has been 12 days since the release of the Mastro report.

“The ultimate tool the committee has is subpoena authority that would compel production of the documents,” Wisniewski said. “We’re willing to wait a moderate amount of time for cooperation,” he said, but added, “The deadline is the end of the week.”

Wisniewski dismissed Handlin’s complaint that the committee has already spent more the $200,000 on legal bills for its special counsel, Reid Schar, the former assistant U.S. Attorney from Illinois who successfully prosecuted Democratic Gov. Rod Blagojevich on corruption charges.

“What is the price of truth?” he asked.

Exhibit F

THE SEDONA CONFERENCE® WORKING GROUP SERIES

wgs℠

THE SEDONA PRINCIPLES: SECOND EDITION

Best Practices Recommendations & Principles for Addressing Electronic Document Production

A Project of The Sedona Conference®
Working Group on Electronic Document
Retention & Production (WG1)

JUNE 2007

The Sedona Conference®

The Sedona Principles (Second Edition) Addressing Electronic Document Production

Editor in Chief: Jonathan M. Redgrave

Executive Editors:
Richard G. Braman
Kenneth J. Withers

Senior Editors:
Thomas Y. Allman
Conor R. Crowley
Ted S. Hiser

Technology Advisor: John H. Jessen

REPRINT REQUESTS:
Requests for reprints or reprint information should be directed to
Richard Braman, Executive Director of The Sedona Conference,
at tsc@sedona.net or 1-866-860-6600.

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference® Working Group 1. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong nor do they necessarily represent official positions of The Sedona Conference®.

The editors wish to thank Jessica Buffenstein and David Degnan for their tireless efforts cite-checking and proofreading.

wgs℠

Copyright © 2007,
The Sedona Conference®

Visit www.thesedonaconference.org

Foreword

Welcome to the Second Edition of *The Sedona Principles: Best Practices Recommendations and Principles for Addressing Electronic Document Production*, a project of The Sedona Conference® Working Group on Best Practices for Electronic Document Retention and Production (WG1). The Sedona Conference® Working Group Series (WGS℠) is designed to bring together some of the nation's finest lawyers, consultants, academics and jurists to address current problems in the areas of antitrust law, complex litigation and intellectual property rights that are either ripe for solution or in need of a "boost" to advance law and policy. (See Appendix D for further information about The Sedona Conference® in general, and the WGS℠ in particular).

Since the first publication of *The Sedona Principles* in January 2004, the *2004 Annotated Version of The Sedona Principles* in the Spring of 2004, and the July 2005 version of *The Sedona Principles,* there have been many developments in the case law as well as significant amendments to the Federal Rules of Civil Procedure and several state civil procedure rules. The Principles, however, have maintained their vitality.

The Second Edition includes updates throughout the Principles and Comments reflecting the new language found in the amended Federal Rules and advances in both jurisprudence and technology. The Introduction has been expanded to include a comparison of *The Sedona Principles* with the amended Federal Rules. Particular attention has been given to updating the language and commentary on Principle 12 (metadata) and Principle 14 (the imposition of sanctions).

The Second Edition has also been rearranged for ease of reference. The 14 Principles themselves are found in the front of this publication, together with a chart cross-referencing each Principle to corresponding sections of the amended Federal Rules of Civil Procedure. In the body of this publication, each rule is followed by one or more Comments, most of which include a "Resources and Authorities" section pointing the reader to selected leading case law, exemplar court rules, and leading legal scholarship for further study.

This version also includes other clerical, minor stylistic, and grammatical edits, as well as updates of the appendices. Since The Sedona Conference® has now published *The Sedona Conference Glossary: E-Discovery and Digital Information Management,* we have eliminated the separate glossary that previously appeared as Appendix A to *The Sedona Principles.*

I want to thank the entire Working Group for all their hard work and contributions, and especially the Editorial Committee and Steering Committee for leading this effort to arrive at the new milestone of a Second Edition! Finally, but certainly not least, the Working Groups of The Sedona Conference could not accomplish their goals without the financial support of the sustaining and annual sponsors of the Working Group Series listed at www.thesedonaconference.org/sponsorship.

Richard G. Braman
Executive Director
The Sedona Conference®
June 2007

The Sedona Principles for Electronic Document Production

Second Edition

1. Electronically stored information is potentially discoverable under Fed. R. Civ. P. 34 or its state equivalents. Organizations must properly preserve electronically stored information that can reasonably be anticipated to be relevant to litigation.

2. When balancing the cost, burden, and need for electronically stored information, courts and parties should apply the proportionality standard embodied in Fed. R. Civ. P. 26(b)(2)(C) and its state equivalents, which require consideration of the technological feasibility and realistic costs of preserving, retrieving, reviewing, and producing electronically stored information, as well as the nature of the litigation and the amount in controversy.

3. Parties should confer early in discovery regarding the preservation and production of electronically stored information when these matters are at issue in the litigation and seek to agree on the scope of each party's rights and responsibilities.

4. Discovery requests for electronically stored information should be as clear as possible, while responses and objections to discovery should disclose the scope and limits of the production.

5. The obligation to preserve electronically stored information requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant electronically stored information.

6. Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information.

7. The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronically stored information were inadequate.

8. The primary source of electronically stored information for production should be active data and information. Resort to disaster recovery backup tapes and other sources of electronically stored information that are not reasonably accessible requires the requesting party to demonstrate need and relevance that outweigh the costs and burdens of retrieving and processing the electronically stored information from such sources, including the disruption of business and information management activities.

9. Absent a showing of special need and relevance, a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual electronically stored information.

10. A responding party should follow reasonable procedures to protect privileges and objections in connection with the production of electronically stored information.

11. A responding party may satisfy its good faith obligation to preserve and produce relevant electronically stored information by using electronic tools and processes, such as data sampling, searching, or the use of selection criteria, to identify data reasonably likely to contain relevant information.

12. Absent party agreement or court order specifying the form or forms of production, production should be made in the form or forms in which the information is ordinarily maintained or in a reasonably usable form, taking into account the need to produce reasonably accessible metadata that will enable the receiving party to have the same ability to access, search, and display the information as the producing party where appropriate or necessary in light of the nature of the information and the needs of the case.

13. Absent a specific objection, party agreement or court order, the reasonable costs of retrieving and reviewing electronically stored information should be borne by the responding party, unless the information sought is not reasonably available to the responding party in the ordinary course of business. If the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information may be shared by or shifted to the requesting party.

14. Sanctions, including spoliation findings, should be considered by the court only if it finds that there was a clear duty to preserve, a culpable failure to preserve and produce relevant electronically stored information, and a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.

Introduction

Discovery in a World of Electronically Stored Information

Discovery, and document production in particular, is a familiar aspect of litigation practice for many lawyers. The explosive growth and diversification of electronic methods for recording, communicating, and managing information has transformed the meaning of the term "document." While twenty years ago PCs were a novelty and email was virtually nonexistent, today more than ninety percent of all information is created in an electronic format.

For courts and lawyers, whose practices are steeped in tradition and precedent, the pace of technological and business change presents a particular challenge.[2] As electronically stored information (often referred to as "ESI") has become more prevalent, courts, litigants, and rule-makers have attempted to meet this challenge, sometimes by applying traditional approaches to discovery, sometimes by turning to treatises (including earlier editions of *The Sedona Principles*), and sometimes by innovating.

Civil litigation in the federal courts is governed by the Federal Rules of Civil Procedure, which were amended in 2006 to include explicit, and in some cases, unique provisions to govern the discovery of electronically stored information.[3] In the main, the Federal Rules are consistent with and reflect the same approach as *The Sedona Principles*. However, there are differences that are discussed in more detail below.

This revised edition of *The Sedona Principles* seeks to synthesize the current and best thinking from the case law and the amended Federal Rules to provide practical standards for modern discovery.[4]

1. What Is Electronic Discovery?

Electronic discovery refers to the discovery of electronically stored information. Electronically stored information includes email, web pages, word processing files, audio and video files, images, computer databases, and virtually anything that is stored on a computing device – including but not limited to servers, desktops, laptops, cell phones, hard drives, flash drives, PDAs and MP3 players. Technically, information is "electronic" if it exists in a medium that can only be read through the use of computers. Such media include cache memory, magnetic disks (such as computer hard drives or floppy disks), optical disks (such as DVDs or CDs), and magnetic tapes. Electronic discovery is often distinguished from "conventional" discovery, which refers to the discovery of information recorded on paper, film, or other media, which can be read without the aid of a computer. Of course, there is also the discovery of tangible "things" which usually refers to physical objects and property.

For readers less familiar with technical terms relevant to electronic discovery, a glossary of terms is provided in *The Sedona Conference Glossary: E-Discovery & Digital Information Management,* which is *available at* http://www.thesedonaconference.org.

[2] "[I]t has become evident that computers are central to modern life and consequently also to much civil litigation. As one district court put it in 1985, '[c]omputers have become so commonplace that most court battles now involve discovery of some computer-stored information.'" Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice & Procedure,* § 2218 at 449 (2d ed. 2006) (quoting *Bills v. Kennecott Corp*., 108 F.R.D. 459, 462 (D. Utah 1985)). Similarly, the *Manual for Complex Litigation* recognizes that the benefits and problems associated with computerized data are substantial in the discovery process. *Manual for Complex Litigation (Fourth)*, § 21.446 (Fed. Jud. Ctr. 2004).

[3] The 2006 amendments to the Federal Rules of Civil Procedure addressing the discovery of electronically stored information became effective December 1, 2006. *See* http://www.uscourts.gov/rules.gov/rules/EDiscovery_w_Notes.pdf. The amendments impact rules 16, 26, 33, 34, 37, 45 and Form 35. For a summary of the new rules and competing viewpoints on their efficacy, see Thomas Y. Allman, *The Impact of the Proposed Federal E-Discovery Rules,* 12 Rich. L. J. & Tech. 13 (2006); Richard L. Marcus, *E-Discovery & Beyond: Toward Brave New World or 1984?* 236 F.R.D. 598, 618 (2006) and Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure,* 4 Nw. J. Tech. & Intell. Prop. 171 (2006), *available at* http://www.northwestern.edu/journals/njtip/v4/n2/3. Unless otherwise indicated, all references to the Federal Rules of Civil Procedure and accompanying Committee Notes are to the language in force December 1, 2006. Shortly after completion of the amendments addressing electronic discovery, the entire Federal Rules of Civil Procedure underwent "restyling," a process intended to clarify and simplify the language and presentation of the rules without affecting their substantive meaning. *See* http://www.uscourts.gov/rules/supct1106/CV_CLEAN_FINAL5-30-07.pdf. The restyled rules are anticipated to go into effect December 1, 2007. While a full analysis of any effect the restyling may have on the interpretation or application of the rules remains for a future date, the Editors wish to point out that the restyling likely will result in one significant nonsubstantive change – Fed. R. Civ. P. 37(f) addressing sanctions for the failure to produce electronically stored information will be renumbered Fed. R. Civ. P. 37(e). See Principle 14, *infra*.

[4] *See Zubulake v. UBS Warburg,* 229 F.R.D. 422, 440 (S.D.N.Y. 2004) (*"Zubulake V"*) (citing the ABA Standards and *The Sedona Principles,* in addition to the evolving revisions to the Federal Rules and local District Rules).

2. How is Discovery of Electronically Stored Information Different?

The answer to the question –"why and how is electronic discovery different?" – lies in the subtle, but sometimes profound, ways in which electronically stored information presents unique opportunities and problems for document production. Magistrate Judge Nan Nolan noted some of these differences in *Byers v. Illinois State Police*, 53 Fed. R. Serv. 3d 740, No. 99 C 8105, 2002 WL 1264004 (N.D. Ill. May 31, 2002):

> Computer files, including emails, are discoverable…However, the Court is not persuaded by the plaintiffs' attempt to equate traditional paper-based discovery with the discovery of email files…Chief among these differences is the sheer volume of electronic information. Emails have replaced other forms of communication besides just paper-based communication. Many informal messages that were previously relayed by telephone or at the water cooler are now sent via email. Additionally, computers have the ability to capture several copies (or drafts) of the same email, thus multiplying the volume of documents. All of these emails must be scanned for both relevance and privilege. Also, unlike most paper-based discovery, archived emails typically lack a coherent filing system. Moreover, dated archival systems commonly store information on magnetic tapes which have become obsolete. Thus, parties incur additional costs in translating the data from the tapes into useable form.

Id. at *31-33.

The qualitative and quantitative differences between producing paper documents and electronic information can be grouped into the following six broad categories.

A. Volume and Duplicability

There is substantially more electronically stored information than paper documents, and electronically stored information is created and replicated at much greater rates than paper documents.

The dramatic increase in email usage and electronic file generation poses particular problems for large data producers, both public and private. A single large entity can generate and receive millions of emails and electronic files each day. A very high percentage of information essential to the operation of public and private enterprises is stored in electronic format and much is never printed to paper. Not surprisingly, the proliferation of the use of electronically stored information has resulted in vast information accumulations. While a few thousand paper documents are enough to fill a file cabinet, a single computer tape or disk drive the size of a small book can hold the equivalent of millions of printed pages. Organizations often accumulate thousands of such tapes as data is stored, transmitted, copied, replicated, backed up, and archived.

Electronic information is subject to rapid and large scale user-created and automated replication without degradation of the data. Email provides a good example. Email users frequently send the same email to many recipients. These recipients, in turn, often forward the message, and so on. At the same time, email software and the systems used to transmit the messages automatically create multiple copies as the messages are sent and resent. Similarly, other business applications are designed to periodically and automatically make copies of data. Examples of these include web pages that are automatically saved as cache files and file data that is routinely backed up to protect against inadvertent deletion or system failure.[5]

[5] Neither the users who created the data nor information technology personnel are necessarily aware of the existence and locations of the copies. For instance, a word processing file may reside concurrently on an individual's hard drive, in a network-shared folder, as an attachment to an email, on a backup tape, in an internet cache, and on portable media such as a CD or floppy disk. Furthermore, the location of particular electronic files typically is determined not by their substantive content, but by the software with which they were created, making organized retention and review of those documents difficult.

B. Persistence

Electronically stored information is more difficult to dispose of than paper documents. A shredded paper document is essentially irretrievable.[6] Likewise, a paper document that has been discarded and taken off the premises for disposal as trash is generally considered to be beyond recovery. Disposal of electronically stored information is another matter altogether. The term "deleted" is misleading in the context of electronic data, because it does not equate to "destroyed." Ordinarily, "deleting" a file does not actually erase the data from the computer's storage devices. Rather, it simply finds the data's entry in the disk directory and changes it to a "not used" status – thus permitting the computer to write over the "deleted" data. Until the computer writes over the "deleted" data, however, it may be recovered by searching the disk itself rather than the disk's directory. This persistence of electronic data compounds the rate at which electronic data accumulates and creates an entire subset of electronically stored information that exists unknown to most individuals with custody and ostensible control over it.

C. Dynamic, Changeable Content

Computer information, unlike paper, has content that is designed to change over time even without human intervention. Examples include: workflow systems that automatically update files and transfer data from one location to another; backup applications that move data from one storage area to another to function properly; web pages that are constantly updated with information fed from other applications; and email systems that reorganize and purge data automatically. As a result, unlike paper documents, much electronically stored information is not fixed in a final form.

More generally, electronically stored information is more easily and more thoroughly changeable than paper documents. Electronically stored information can be modified in numerous ways that are sometimes difficult to detect without computer forensic techniques. Moreover, the act of merely accessing or moving electronic data can change it. For example, booting up a computer may alter data contained on it. Simply moving a word processing file from one location to another may change creation or modification dates found in the metadata. In addition, earlier drafts of documents may be retained without the user's knowledge.

D. Metadata

A large amount of electronically stored information, unlike paper, is associated with or contains information that is not readily apparent on the screen view of the file. This additional information is usually known as "metadata." Metadata includes information about the document or file that is recorded by the computer to assist in storing and retrieving the document or file. The information may also be useful for system administration as it reflects data regarding the generation, handling, transfer, and storage of the document or file within the computer system. Much metadata is neither created by nor normally accessible to the computer user.

There are many examples of metadata. Such information includes file designation, create and edit dates, authorship, comments, and edit history. Indeed, electronic files may contain hundreds or even thousands of pieces of such information. For instance, email has its own metadata elements that include, among about 1,200 or more properties, such information as the dates that mail was sent, received, replied to or forwarded, blind carbon copy ("bcc") information, and sender address book information. Typical word processing documents not only include prior changes and edits but also hidden codes that determine such features as paragraphing, font, and line spacing. The ability to recall inadvertently deleted information is another familiar function, as is tracking of creation and modification dates.

[6] Modern technology, however, has made recovery at least a theoretical possibility. *See* Douglas Heingartner, *Back Together Again,* New York Times, July 17, 2003, at G1 (describing technology that can reconstruct cross-shredded paper documents).

Similarly, electronically created spreadsheets may contain calculations that are not visible in a printed version or hidden columns that can only be viewed by accessing the spreadsheet in its "native" application, that is, the software application used to create or record the information. Internet documents contain hidden data that allow for the transmission of information between an internet user's computer and the server on which the internet document is located. So-called "meta-tags" allow search engines to locate websites responsive to specified search criteria. "Cookies" are text files placed on a computer (sometimes without user knowledge) that can, among other things, track usage and transmit information back to the cookie's originator.[7]

Generally, the metadata associated with files used by most people today (such as Microsoft Office™ documents) is known as "application metadata." This metadata is embedded in the file it describes and moves with the file when it is moved or copied. On the other hand, "system metadata" is not embedded within the file it describes but stored externally. System metadata is used by the computer's file system to track file locations and store information about each file's name, size, creation, modification, and usage.

Understanding when metadata is relevant and needs to be preserved and produced represents one of the biggest challenges in electronic discovery. Sometimes metadata is needed to authenticate a disputed document or to establish facts material to a dispute, such as when a file was accessed in a suit involving theft of trade secrets. In most cases, however, the metadata will have no material evidentiary value – it does not matter when a document was printed, or who typed the revisions, or what edits were made before the document was circulated. There is also the real danger that information recorded by the computer as application metadata may be inaccurate. For example, when a new employee uses a word processing program to create a memorandum by using a memorandum template created by a former employee, the metadata for the new memorandum may incorrectly identify the former employee as the author. However, the proper use of metadata in litigation may be able to provide substantial benefit by facilitating more effective and efficient searching and retrieval of electronically stored information.

E. Environment-Dependence and Obsolescence

Electronic data, unlike paper data, may be incomprehensible when separated from its environment.[8] For example, the information in a database may be incomprehensible when removed from the structure in which it was created. If the raw data (without the underlying structure) in a database is produced, it will appear as merely a long list of undefined numbers. To make sense of the data, a viewer needs the context, including labels, columns, report formats, and similar information. Report formats, in particular, allow understandable, useable information to be produced without producing the entire database. Similarly, stripping metadata and embedded data from data files such as spreadsheets can substantially impair the functionality of the file and the accuracy of the production as a fair representation of the file as kept and used in the ordinary course of business.

Also, it is not unusual for an organization to undergo several migrations of data to different platforms within a few years. Because of rapid changes in computer technology, neither the personnel familiar with the obsolete systems nor the technological infrastructure necessary to restore the out-of-date systems may be available when this "legacy" data needs to be accessed. In a perfect world, electronically stored information that has continuing value for business purposes or litigation would be converted for use in successor systems, and all other data would be discarded. In reality, such migrations are rarely flawless.

[7] There is much confusion over the use of terms and distinctions between application and systems metadata can be confusing. *See* Craig Ball, *Understanding Metadata: Knowing Metadata's Different Forms and Evidentiary Significance Is Now an Essential Skill for Litigators,* 13 Law Tech. Prod. News 36 (Jan. 2006).

[8] In addition, passwords, encryption, and other security features can limit the ability of users to access electronic documents.

F. Dispersion and Searchability

While a user's paper documents will often be consolidated in a handful of boxes or filing cabinets, the user's electronically stored information may reside in numerous locations – desktop hard drives, laptop computers, network servers, floppy disks, flash drives, CD-ROMS, DVDs and backup tapes. Many of these electronic documents may be identical backup or archive copies. However, some documents may be earlier versions drafted by that user or by other users who can access those documents through a shared electronic environment.

Consequently, it may be more difficult to determine the provenance of electronically stored information than paper documents. The ease of transmitting electronic data and the routine modification and multi-user editing process may obscure the origin, completeness, or accuracy of a document. Electronic files are often stored in shared network folders that may have departmental or functional designations rather than author information. In addition, there is growing use of collaborative software that allows for group editing of electronic data, making authorship determination more difficult. Finally, while electronically stored information may be stored on a single location, such as a local hard drive, it is likely that such documents may also be found on high-capacity, undifferentiated backup tapes, or on network servers—not under the custodianship of an individual who may have "created" the document.

While the dispersed nature of electronically stored information complicates discovery, the fact that many forms of electronically stored information and media can be searched quickly and accurately by automated methods provides new efficiencies and economies. In many instances, software is able to search far greater volumes of these types of electronically stored information than human beings could review manually.

3. What Are *The Sedona Principles* and How Have They Influenced the Evolution of E-Discovery?

The reliance upon discovery of electronically stored information has increased markedly in the last decade, although indications of its growing importance to civil litigation have been apparent since the early 1980s.

The Sedona Principles are at the heart of two major parallel developments, one involving the identification and articulation of "best practices" and the other involving rulemaking. The *Principles* evolved from discussions involving wide segments of the parties affected by and deeply involved in the actual e-discovery practice and represent a consensus viewpoint. They evolved into "final" form by 2004. The focus on best-practice guidelines is also embodied in the American Bar Association's "Civil Discovery Standards" and the Conference of Chief Justices' "Guidelines for State Trial Courts." On the rulemaking front, early developments at the state level[9] were followed by the work of the Advisory Committee on Civil Rules of the Judicial Conference of the United States, beginning in 2000, to explore the need for targeted rulemaking. That effort resulted in the 2006 amendments to the Federal Rules of Civil Procedure (the "amended Federal Rules" or the "2006 amendments"). Since the adoption of the amended Federal Rules, a number of states have begun to consider whether to adopt some form of e-discovery rules or guidelines. Many appear to be awaiting the consequences of the federal amendments. Other states require or encourage early discussions of preservation issues and identification of key sources of electronically stored information.[10] An effort by the Uniform Law Commissioners to promote uniform rulemaking modeled on the amended Federal Rules is also underway.

The Sedona Principles have an impressive track record of providing useful assistance to individual federal and state courts facing novel e-discovery issues. They have been influential in providing intellectual support in a number of precedent-

[9] The State of Texas was the first state to enact formal e-discovery rules, having added Rules §§196.3 and 196.4 to its Rules of Civil Procedure in 1999. The State of Mississippi enacted a similar rule in 2003.

[10] *See* New York Rules for the Commercial Division of the Supreme Court, §202.70(g).

setting cases involving preservation obligations,[11] search methodology,[12] production of metadata[13] and the handling of privileged information,[14] to name only a few examples.

We anticipate that the role of providing guidance and best practices will continue to be the province of *The Sedona Principles* – a process illustrated by the changes in Principles 12 (metadata) and 14 (sanctions), as well as the expanded commentary under all fourteen principles. Indeed, there are efforts underway to adopt similar principles in Canada and other countries.[15]

4. What is the Relationship Between *The Sedona Principles* and Court Rules?

A. Federal Rules of Civil Procedure

The Sedona Principles helped shape the legal environment in which the amended Federal Rules were drafted and adopted. In turn, the 2007 revision of *The Sedona Principles* is heavily influenced by consideration of the amended Federal Rules. This interplay between *The Sedona Principles* and the amended Federal Rules will continue. However, *The Sedona Principles* address a number of key topics that the amendments do not. For example, civil procedure rules only apply once litigation commences, and are procedural and not substantive. Therefore the amended Federal Rules do not establish standards governing pre-litigation preservation.[16] *The Sedona Principles* cover the topic in several best practice standards which continue to play a major role in the developing national consensus on the topic.[17]

In many respects, the processes and procedures adopted in the amended Federal Rules and *The Sedona Principles* are consistent. A summary chart comparing *The Sedona Principles* and the amended Federal Rules, by key topics, is found in the front of this publication.

(i) Scope of Discovery of Electronically Stored Information. Amended Federal Rule 34 now provides for the discovery[18] of "electronically stored information" as well as documents and tangible things. This clarification of the scope of discovery parallels Sedona Principle 1 that electronic information of all forms and in all media is potentially subject to discovery. For consistency, the Working Group has adopted the phrase "electronically stored information" for use throughout *The Sedona Principles* in order to employ terminology that is consistent with the Rules.[19]

[11] *Consolidated Aluminum Corp. v. Alcoa, Inc.*, No. 03-1055-C-M2, 2006 WL 2583308, at *6 n. 18 (M.D. La. July 19, 2006) (relying on *The Sedona Principles* in determining scope of preservation obligation).

[12] *Treppel v. Biovail,* 233 F.R.D. 363 (S.D. N.Y. 2006) (relying on *The Sedona Principles* in determining appropriateness of defined search strategies required).

[13] *Williams v. Sprint/United Management Co.,* 230 F.R.D. 640 (D. Kan. 2005) (relying on *The Sedona Principles* in determining whether production of metadata was required).

[14] *Hopson v. The Mayor and City Council of Baltimore,* 232 F.R.D. 228, 234 (D. Md. 2005) (relying on *The Sedona Principles* in establishing protocol for privileged document clawback agreement).

[15] *See The Sedona Canada Principles* (A Project of The Sedona Conference Working Group 7 (WG7)) (February 2007 Public Comment Draft) *available at* http://www.thesedonaconference.org.

[16] Thomas Y. Allman, *Rule 37(f) Meets Its Critics: The Justification for A Limited Safe Harbor for ESI,* 5 Nw. J. Tech. & Intell. Prop. 1 (2006).

[17] *See* Sedona Principle 5 (a party must act reasonably and in good faith in executing preservation obligations, but is not expected to take every conceivable step). Other principles dealing with preservation obligations are Principle 3 (early discussion); 6 (presumptions regarding responding parties); 8 (disaster recovery backup tapes); 9 (deleted, shadowed, fragments or residual data); 12 (metadata) and 14 (sanctions for failure to preserve).

[18] Fed. R. Civ. P. 26(a)(1), which requires "initial disclosures" independent of the Rule 34 discovery request process, also includes an obligation to disclose electronically stored information which a party intends to use to support its claims or defenses.

[19] Even before "electronically stored information" was explicitly added to Rule 34, it was "black-letter law that computerized data is discoverable if relevant." *Anti-Monopoly, Inc. v. Hasbro, Inc.,* No. 94 Civ. 2120, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995); *see also Bills v. Kennecott Corp.,* 108 F.R.D. 459, 463-64 (D. Utah 1985) ("[I]nformation stored in computers should be as freely discoverable as information not stored in computers.").

(ii) Limits on Required Production (General). All discovery – including discovery of electronically stored information – is subject to the proportionality limits set forth in Rule 26(b)(2)(C), which require a court to weigh the potential benefit or importance of requested information against the burden on the party that would have to produce the documents.[20] Rule 26(b)(2)(C)(iii) provides for limiting discovery when "the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues." Rule 26(b)(2)(C)(i) provides that discovery may be limited if "the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive." The Federal Rules are intended to protect parties from unduly burdensome, unnecessary, or inefficient discovery. Rule 26(b)(1) limits discovery to matters, not privileged, which are relevant to a claim or defense.

The Sedona Principles reflect these limits in Principle 2, which provides that "the technological feasibility and realistic costs of preserving, retrieving, reviewing, and producing electronically stored information" should be taken into account in achieving balance. Principle 6 acknowledges and expands the concept by noting that "responding parties are best situated" to evaluate the appropriate procedures, methodologies and technologies to preserve and produce their electronically stored information.

(iii) Limits on Discovery Based on Accessibility. Rule 26(b)(2)(B) establishes a two-tiered approach to discovery unique to the production of electronically stored information. Relevant electronically stored information that resides on sources that are identified as "not reasonably accessible because of undue burden or cost" may be withheld from production, without resort to a court order, provided there is an appropriate identification of the sources of electronically stored information that are not being produced. If the producing party can sustain the burden of demonstrating the undue burden or costs on a challenge, the requesting party then has the burden to show "good cause" for production from these sources.[21] Cost-shifting may be ordered as a condition of production.

Sedona Principle 8 also suggests an initial presumptive limit on discovery, but relates the limit on the initial scope of discovery for relevant evidence to the actual use of information in a business. Sedona Principle 8 states that the "primary source" for discovery should be "active data and information." The commentary to Principle 8 harmonizes the two approaches.

(iv) Protective Orders and Cost-Shifting. Rule 26(c) allows a court to enter a protective order against burdensome discovery and historically is the source of the authority to shift costs for all forms of discovery. The 2006 amendments reinforce this by adding a provision in Rule 26(b)(2)(B) that a producing party may seek a protective order to test its obligations to preserve or produce electronically stored information.

Unlike the Federal Rules, Sedona Principle 13 explicitly states that the costs of "retrieving and reviewing" electronically stored information that is not "reasonably available" may be shifted to the requesting party. The revised commentary under Principle 13 addresses the differences, as well as distinction, between cost shifting under Rule 26(b)(2)(B) and Rule 26(c).

[20] *See In re Microcrystalline Cellulose Antitrust Litig*., 221 F.R.D. 428, 429 (E.D. Pa. 2004) (applying limits of Rule 26 (b)(2) (prior to renumbering) to limit unreasonable demand for sales data not needed in antitrust action).

[21] Ordinarily a requesting party should obtain and evaluate the information from accessible sources before insisting that the responding party search and produce from sources that are not reasonably accessible. *See* Fed. R. Civ. P. 26(b) Committee Note.

(v) Mandatory Early Discussions. The Rule 26(f) requirement for an early "meet and confer" prior to the Rule 16 scheduling conference has been substantially strengthened and expanded in a manner similar to that advocated by Sedona Principle 3.[22] Parties are now expected to have early and meaningful discussions of "any issues relating to preserving discoverable information" and to develop a proposed discovery plan that takes into account "disclosure or discovery" of electronically stored information including, but not limited to, both the form of production and the method of handling claims of privilege after production.

(vi) Form of Production and Metadata. Electronically stored information is created in a form "native" to that application and computer system, together with system and application metadata. This electronically stored information may be produced in a variety of forms other than its "native" form. Some forms of production replicate the view of the user and provide other capabilities such as searchability, but with limited or no metadata or embedded data. The Advisory Committee rejected proposals to mandate any particular form of production and did not take a position on the need to produce metadata. Rule 26(f) instead emphasizes the need to discuss this topic early to attempt to reach agreement, and Rule 34(b) provides a process for resolving disputes, while providing two alternative forms of production in the event the parties do not reach agreement or a court order is not entered: the form or forms "in which it is ordinarily maintained" or "in a form or forms that are reasonably usable."

The phrase "ordinarily maintained" is not synonymous with "native format." It is common for electronic information to be migrated to a number of different applications and formats in the ordinary course of business, particularly if the information is archived for long-term storage. Routine migration will likely result in the loss or alteration of some elements of metadata associated with the native application, and the addition of new elements. Given the variety of forms in which electronically stored information is found and the many options available in producing it, a difference may exist between the form in which electronically stored information is preserved and that in which it is produced for use, depending upon the issues involved and the preferences of the parties or any agreements or orders pending production.[23]

Sedona Principle 12, in contrast, deals directly with the issue of the need to preserve and produce metadata. It has been amended in this 2007 Version to provide more explicit guidance regarding issues relating to both the relevance and usability of metadata. Previously, Principle 12 only provided guidance on a narrow aspect of the metadata issue.[24]

(vii) Inadvertent Production of Privileged or Work Product Information. Because of the tremendous volume of electronically stored information that may need to be reviewed in response to a discovery request, and the complex nature of the information itself, which may contain metadata, embedded data, and non-obvious contextual links, reviewing electronically stored information for privilege is particularly difficult. Even the most diligent review is likely to result in some inadvertent production of privileged information. Serious practical and ethical issues exist when privileged information is inadvertently produced during discovery, not the least of which is the potential waiver under applicable law.[25] Because rules of procedure cannot enlarge or abridge substantive rights, including the substantive law of privilege and waiver, the amended Federal Rules only create a procedure by which parties are now required, by Rule 26(f), to conduct an early discussion of the possible

[22] *See* Sedona Principle 3, which states: "Parties should confer early in discovery regarding the preservation and production of electronic data and documents when these matters are at issue in the litigation, and seek to agree on the scope of each party's rights and responsibilities." Mandatory early discussion of contentious e-discovery issues was enthusiastically endorsed by many who testified at the Public Hearings in early 2005. The Testimony and filed Comments of almost 200 witnesses are accessible from the U.S. Courts website ("Comments"). *See* 2004 Civil Rules Committee Chart, including Request to Testify, *available at* http://www.uscourts.gov/rules/e-discovery.html. The Comments represent a valuable snapshot of e-discovery concerns and practices as of 2005 and contain many insightful observations.

[23] *See In re Priceline.Com Inc. Securities Litig.*, 233 F.R.D. 88, 89-91 (D. Conn. 2005) (resolving disputes over the form of preservation and production by ordering that production be in TIFF and PDF form but that the original data be maintained in its original native file format for the duration of the litigation).

[24] Sedona Principle 12 formerly focused on the need for the test of materiality in determining if preservation and production of metadata was needed. As implied in the *Priceline.Com* opinion, *supra*, it may be advisable to distinguish between the file format used in preservation and the form or forms used for production.

[25] Jonathan M. Redgrave and Kristin M. Nimsger, *Electronic Discovery and Inadvertent Productions of Privileged Documents,* 49 Fed. Law. 37 (July 2002).

need for voluntary agreements to govern the treatment of a post-production privilege claim. Any agreement on the topic may be included in the Rule 16(b) Scheduling Order, but the Committee Notes recognize that such agreements between the parties, even if embodied in a court order, may not bind non-parties, a controversial subject being addressed by the Advisory Committee on the Rules of Evidence.[26] Rule 26(b)(5)(C) provides a standard procedure by which parties can identify and retrieve inadvertently produced documents and electronically stored information. It also sets forth a procedure by which the receiving party can challenge the privilege assertion.

Sedona Principle 10 is consistent with this approach, emphasizing the need for reasonable, mutually agreed-upon procedures to protect privileges and objections to production. Importantly, revisions to comment 10.d help to define and distinguish two common categories of agreements, the "clawback" and the "quick peek."

(viii) Sanction Limitations. The 2006 amendments do not directly address the nature and extent of preservation obligations. Instead, new Rule 37(f) limits the availability of rule-based sanctions when electronically stored information has been "lost as a result of the routine, good faith operation of an electronic information system."

While Rule 37(f) does not purport to limit the power to issue sanctions under a court's inherent power, this provision represents a considered policy decision intended to prevent unreasonable and unnecessary interruption of routine information systems during discovery.[27] *The Sedona Principles* do not include a directly comparable provision to Rule 37(f). Instead, Sedona Principle 14 focuses on the underlying issue – the elements required to justify the imposition of sanctions. The nature and extent of preservation obligations are discussed in general respects in Principles 1 and 5, with specific examples of how they apply in Principles 6, 7, 8, 9, 11 and 12.

A slight change in Principle 14 has been made in the 2007 version to more closely conform the culpability element in Principle 14 to emerging case law and to reflect the influence of the policy decision underlying Rule 37(f).[28]

(ix) Third Party Discovery. The obligations and protections added by the 2006 amendments generally apply to discovery of third parties. *See* Fed. R. Civ. P. 45. *The Sedona Principles* do not expressly distinguish between discovery of parties and non-parties, although the commentary does reflect the different treatment of non-parties versus parties in terms of evaluating burdens.

B. State Rules

The volume of reported e-discovery decisions has been smaller in state courts, leading to the misperception that electronic discovery was more prevalent in the types of disputes brought into federal court. As recently as a few years ago, outside the hotly contested areas of divorce law and employment disputes, few reported state court decisions existed. This is quickly changing as electronic discovery becomes more commonplace in state court litigation. *The Sedona Principles* have played a major role in these early cases.[29]

[26] Proposed Evidence Rule 502, currently under consideration by the Advisory Committee Evidence Rules, addresses the impact on third parties of non-waiver agreements approved by the courts, among other topics. The proposed rule was approved by the Advisory Committee on Evidence on April 13, 2007, *available at* http://www.uscourts.gov/rules/Excerpt_EV_Report_Pub.pdf#page=4 .

[27] *Turner v. Resort Condos. Int'l LLC,* No. 1:03-cv-2025, 2006 WL 1990379, at *8 (S.D. Ind. July 13, 2006) (refusing to issue sanctions for alleged failures in preservation where there was no bad faith alteration or destruction of evidence).

[28] The clarification has been made that "grossly negligent" conduct can support sanctions for inadequate conduct in searching for discoverable information. *See Phoenix Four, Inc. v. Strategic Resources Corp.,* No. 05 Civ. 4837(HB), 2006 WL 1409413, at *9 (S.D.N.Y. May 23, 2006) (sanctioning party and counsel for failure to adequately search former servers used by defendant).

[29] *See Bank of America Corp. v. SR Int'l Bus. Ins. Co.,* No. 05-CVS-5564, 2006 WL 3093174 (N.C. Super. Ct. Nov. 1, 2006).

It is by no means certain that the 2006 amendments to the Federal Rules will be adopted in the majority of the states. Rules of civil procedure are promulgated by the highest court in each state, based on input from committees or, in some cases, by action (or inaction) of legislative bodies.[30] Historically, while amendments to the Federal Rules of Civil Procedure have been highly influential on state procedural rulemaking, in recent years the benefits of uniformity have been questioned.[31] To some extent, this can be attributed to the frequency of changes in the rules and some unpopular experimentation, including the addition of mandatory disclosures in the 1993 rule amendments, modified in the 2000 amendments.

Two national initiatives are directed at promoting uniformity among the state trial courts. Both have been heavily influenced by *The Sedona Principles.* The first effort, which eschews formal rulemaking, is that of the Conference of Chief Justices ("CCJ") which has issued "Guidelines for State Trial Courts on Discovery of Electronically Stored Information" (August, 2006) (the "Guidelines").[32] The avowed purpose of the Guidelines is to provide "a reference document to assist state courts in considering issues related to electronic discovery," but not to supplant the rulemaking process of individual states ("[t]he Guidelines should not be treated as model rules that can simply be plugged into a state's procedural scheme"). The effort may be leading to some success at the state level.[33]

The second effort is that of the Electronic Discovery Committee of the National Conference of Commissioners on Uniform Laws ("NCCUSL") to develop uniform model discovery rules for adoption in the states.[34] Although still in draft form as of this writing, the effort to date has been closely modeled on the federal amendments.

5. Why Do Courts and Litigants Need Sedona Best Practice Standards Tailored to E-Discovery?

With the advent of the 2006 amendments to the Federal Rules, the dramatic growth in case law, and the increased number of best-practice guidelines such as those authored by the Conference of Chief Justices and the National Uniform Law Commissioners, it is fair to ask about the role remaining for best-practice standards like *The Sedona Principles*. The Federal Rules are necessarily procedural and cannot provide the level of detail found in *The Sedona Principles*.

Cases are necessarily fact specific. The Rules and Guidelines are not self-executing. A significant role likely remains for the evolution of current, authoritative best-practice standards and principles such as *The Sedona Principles* to provide guidance in the interpretation and application of electronic discovery rules and case law**.**

The Working Group began to examine the issue of electronic document production closely in 2002, focusing both on its similarities to and differences from paper document production. The principles and commentary that follow, as revised in 2007 Second Edition, reflect our continuing efforts to assist the reasoned and just evolution of the law as it relates to the preservation and production of electronically stored information.

[30] *See* Linda S. Mullenix, *The Varieties of State Rulemaking Experience and the Consequences for Substantive Procedural Fairness* and *Table – State Rulemaking Authorities,* Roscoe Pound Institute 2005 Forum for State Appellate Court Judges, *available at* www.roscoepound.org/new/updates/2005Forum.htm.

[31] *See* Stephen N. Subrin, *Federal Rules, Local Rules, and State Rules: Uniformity, Divergence, and Emerging Procedural Patterns,* 137 U. Pa. L. Rev. 1999 (1989) (movement leading to passage of Rules Enabling Act motivated in part by need for uniformity among courts prompted by the changes compelled by "the telephone, telegraph, train, and airplane").

[32] The Conference of Chief Justices, *Guidelines for State Courts Regarding Discovery of Electronically Stored Information* (Aug. 2006), *available at* http://www.ncsconline.org/WC/Publications/CS_ElDiscCCJGuidelines.pdf.

[33] *See Bank of America Corp., supra* note 29.

[34] Information on the current status of the uniform model discovery rules is found at http://www.nccusl.org/Update/CommitteeSearchResults.aspx?committee=248.

12. Absent party agreement or court order specifying the form or forms of production, production should be made in the form or forms in which the information is ordinarily maintained or in a reasonably usable form, taking into account the need to produce reasonably accessible metadata that will enable the receiving party to have the same ability to access, search, and display the information as the producing party where appropriate or necessary in light of the nature of the information and the needs of the case.

Comment 12.a. Metadata

An electronic document or file usually includes not only the visible text but also hidden text, formatting codes, formulae, and other information associated with the file. These many types of ancillary information are often lumped together as "metadata," although some distinctions between different types of metadata should be recognized.

For example, the two most common distinctions are between "application" metadata and "system" metadata. Application metadata is created as a function of the application software used to create the document or file. Common application metadata instructs the computer how to display the document (for example, the proper fonts, spacing, size, and color). Other application metadata may reflect modifications to the document, such as prior edits or editorial comments. This metadata is embedded in the file it describes and moves with the file when it is moved or copied. System metadata reflects information created by the user or by the organization's information management system. Such information may, for example, track the title of the document, the user identification of the computer that created it, the assigned data owner, and other document "profile" information. System metadata generally is not embedded within the file it describes, but is stored externally elsewhere on the organization's information management system. Depending on the circumstances of the case, the content value of a particular piece of metadata may be critical or may be completely irrelevant. It may be important, therefore, when planning the scope of discovery to determine the types and locations of metadata associated with the various application data types that will be targeted in the discovery and determine whether or not they may play an ongoing role.

Aside from its potential relation to the facts of the case, metadata may also play a functional role in the usability of electronically stored information. For example, system metadata may allow for the quick and efficient sorting of a multitude of files by virtue of the dates or other information captured in metadata. In addition, application metadata may be critical to allow the functioning of routines within the file, such as cell formulae in spreadsheets.

Care should be taken when using metadata, as the content of a given piece of metadata may convey information that is contextually inaccurate. For example, when a Microsoft Word™ document is created, the computer on which that document is saved may automatically assign the document an "author" based on the information available on that computer. That document may be used as a template by other persons, but the "author" information is never changed. Thus, subsequent iterations of the document may carry as an "author" a person with no knowledge of the content of the document. Accordingly, a proper and thorough analysis should be undertaken in order to properly assess how the metadata was created.

The extent to which metadata should be preserved and produced in a particular case will depend on the needs of the case. Parties and counsel should consider: (a) what metadata is ordinarily maintained; (b) the potential relevance of the metadata to the dispute (e.g., is the metadata needed to prove a claim or defense, such as the transmittal of an incriminating statement); and (c) the importance of reasonably accessible metadata to facilitating the parties' review, production, and use of the information. In assessing preservation, it should be noted that the failure to preserve and produce metadata may deprive the producing party of the opportunity later to contest the authenticity of the document if the metadata is material to that determination. Organizations should evaluate the potential benefits of retaining native files and metadata (whether or not it is produced) to ensure that documents are authentic and to preclude the fraudulent creation of evidence.[37]

RESOURCES AND AUTHORITIES

Shira A. Scheindlin and Jonathan M. Redgrave, *Discovery of Electronic Information, 2 Bus. & Commerical Litig. in Fed. Courts,* §22:22 (Robert L. Haig ed., 2005 & Supp. 2006).

Kentucky Speedway, LLC v. NASCAR, Inc., Civ. No. 05-138-WOB, 2006 W.S. Dist. Lexis 92028 (E.D. Ky. Dec. 18, 2006) (court declines to require defendant to supplement production of electronically stored information, relying on a perceived emerging presumption against the production of metadata and citing Sedona Principle 12 (2005 edition)).

In re Priceline.com Inc. Sec. Litig., 233 F.R.D. 88, 91 (D. Conn. 2005) ("Defendants shall produce responsive information contained in stored data files to plaintiffs in TIFF or PDF form with Bates numbering and appropriate confidentiality designations, shall produce searchable metadata databases, and shall maintain the original data itself in native format for the duration of the litigation.").

Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 643 (D. Kan. 2005) (*"Williams I"*)(finding that if production of spreadsheets are ordered to be produced in form in which they are maintained, metadata should be produced, citing *The Sedona Principles* for definition and discussion of metadata).

Comment 12.b. Formats used for collection and production: "ordinarily maintained" v. "reasonably usable"

Electronically stored information is fundamentally different from paper information in that it is dynamic, created and stored in myriad different forms, and contains a substantial amount of nonapparent data. Because of these differences, approaching the production of electronically stored information as though it is just the modern equivalent of a paper document collection will likely lead to a failure to fully consider the complex issues involved and a failure to select the most relevant and functional form of production for a particular type of electronic information.

[37] Several attorney disciplinary bodies have issued opinions on the dangers of counsel inadvertently transmitting attorney-client confidences as metadata embedded within electronic documents and the efficacy of receiving counsel searching for and viewing such metadata. *See, e.g.*, New York Ethics Op. 749 (2001); ABA Comm. on Ethics And Prof'l Responsibility, Formal Op. 06-442; New York Ethics Op. 749 (2001); Maryland Bar Assoc. Comm. on Ethics Op. 2007-09. The Working Group expresses no opinion on these decisions, and it should be noted that the issues discussed in these opinions usually arise in a transactional context, before any duty to preserve electronically stored information relevant to anticipated or pending litigation arises. In transactional settings, counsel is free to routinely employ so-called "metadata scrubbers" to remove unwanted metadata before transmitting electronic documents to clients or to other counsel. In deciding to do so, counsel should weigh the dangers of transmitting client confidences or attorney-client communication against the benefits that metadata provides for later document management, indexing and review, and may choose to "scrub" only certain categories of particularly sensitive metadata. Once litigation is anticipated, however, routine metadata scrubbing of relevant documents must be reexamined in light of the preservation duty.

Electronic information is created and stored by a computer in a file format "native" to the software application used to create or utilize the information. However, electronically stored information can be produced in any number of formats, some more useful than others. For example, although an email message may be readily understood when presented as plain text printed on paper, this is not the case with audio or video files. All electronic documents and files, to one extent or another, contain information that is not apparent when displayed on a screen, printed on paper, or heard on speakers. The extent to which a production of electronically stored information includes such data depends on the form of production. For example, electronic information produced in the form in which the file was created (or "native format") will contain application metadata such as formulae in spreadsheets or "tracked changes" in word processing documents.

An electronic document or file produced in native format may also be accompanied by system metadata, such as the date the file was created or the identity of the computer on which it was created. However, electronic information produced in a static, two-dimensional form, such as an image file (e.g., TIFF or PDF, explained below), while having some practical advantages, does not contain any of the original metadata. Certain types of electronic information, such as databases, simply cannot be converted from their native, dynamic, three-dimensional form without significant loss of information and functionality.

Accordingly, there should be two primary considerations in choosing the form of production: (1) the need for, or probative value of both apparent and metadata; and (2) the extent to which the production of metadata will enhance the functional utility of the electronic information produced and allow the parties to conduct a more cost-effective and efficient review. These considerations should be weighed against the negative aspects associated with each format.[38] For example, production in a "native" format entails both advantages and disadvantages. Native production, which generally includes the entire file and associated metadata, may afford the requesting party access to the same information and functionality available to the producing party and, from a technical perspective, usually requires minimal processing before production. However, information produced natively may be difficult or impossible to redact or Bates number, and files in their native forms must be viewed using applications capable of opening and presenting the information without alteration. Suitable applications are not always accessible to requesting parties, who may also lack the equipment or expertise required to use such applications.

A native file production that includes a substantial volume and variety of file types could become very expensive and burdensome for the requesting party. In addition, since certain metadata could contain or reveal privileged, secret, or other sensitive information, an organization may determine that it must review such metadata before producing it, which can substantially impact the speed of production.

In current practice, many parties, local rules and courts have endorsed the use of image production formats, principally the Tagged Image File Format ("TIFF") and Adobe Portable Document Format ("PDF") formats. Standing by themselves, image file productions are the equivalent of printed pages from the screen. They have the advantage of a static format that can be Bates numbered and redacted, and, compared to native files, it is harder (but not impossible) to alter the data inadvertently or deliberately. However, simple image productions require significant processing that is time consuming and costly. The image productions, by themselves, also lose searchable text and metadata that might enable better understanding and utility of the evidence.

In an effort to replicate the usefulness of native files while retaining the advantages of static productions, image format productions are typically accompanied by "load files," which are ancillary files that may contain textual content and relevant system metadata. Again, however, there are potentially significant costs inherent in this process, and it does not work well for certain types of electronically stored information such as spreadsheets and dynamic databases.

[38] *See The Sedona Canada Principles,* Principle 8, Comment 8.b (2006), *available at* http://www.thesedonaconference.org.

The routine preservation of metadata pending agreements or decisions on the ultimate form of production may be beneficial in a number of ways. Preservation of metadata may provide better protection against inadvertent or deliberate modification of evidence by others and the systematic removal or deletion of certain metadata may involve significant additional costs that are not justified by any tangible benefit. Moreover, the failure to preserve and produce metadata may deprive the producing party of the opportunity later to contest the authenticity of the document if the metadata would be material to that determination.

In amending Rule 34(b) to accommodate the production of electronically stored information, the Advisory Committee acknowledged that wherever possible, parties should first attempt to reach agreement on the various form or forms of production, given that different types of data may serve different purposes and the need for native production and metadata may vary. The Advisory Committee also recognized that the default forms of production appropriate to paper discovery did not have direct equivalents in electronic discovery. However, the goals furthered by providing default forms of production governing paper discovery should be the same in electronic discovery – to encourage forms of production that would be inexpensive for the producing party and reasonably useable for the requesting party; and to avoid costly data conversion on the one hand, and the electronic equivalent of the "document dump" on the other hand. Therefore, without mandating any particular form of production, Rule 34(b) provides that in the absence of agreement or a specific court order, a producing party should produce electronically stored information either in the form in which it is "ordinarily maintained" or in a "reasonably usable" form.

The form in which electronically stored information is "ordinarily maintained" is not necessarily synonymous with the form in which it was created. There are occasions when business considerations involve the migration or transfer of electronically stored information to other applications or systems. For example, customer information may routinely be gathered by an organization from Internet-based forms, then collected in a relational database for further business use. The information may be incorporated into Microsoft Word™ documents, such as memoranda or correspondence, which may later be transferred into static electronic images for long-term storage and retrieval. In such cases, the form in which the electronically stored information is maintained understandably varies from that in which it was obtained or created. Absent an attempt to deliberately downgrade capabilities or characteristics for the purposes of avoiding obligations during specific litigation, migration to alternative forms for business purposes is not considered inconsistent with preservation obligations.

What constitutes a "reasonably usable" form will depend on the circumstances of a case, given that the need for email, documents, spreadsheets, or dynamic databases can all vary. As noted earlier, selection of a "reasonably usable" form is best handled by an agreement between the parties regarding the distinct categories of electronically stored information sought in a case. But where such an agreement is not reached, the Committee Note to Rule 34(b) explicitly states that "[i]f the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature." Accordingly, a party should produce electronically stored information in "reasonably usable" forms, though not necessarily "native format."

In determining the appropriate forms of production in a case, requesting parties and counsel should consider: (a) the forms most likely to provide the information needed to establish the relevant facts of the case; (b) the need for metadata to organize and search the information produced; (c) whether the information sought is reasonably accessible in the forms requested; and (d) the requesting party's own ability to effectively manage and use the information in the forms requested.

Producing parties and counsel should consider: (a) the relative risks of inadvertent production of confidential, privileged, and work product information associated with different forms of production; (b) difficulties in redaction, tracking, and use of native files; (c) whether alternative (e.g., "nonnative") forms of production provide sufficient usability (e.g., by providing adequate accompanying information through load files) such that the producing and requesting parties have the same access to functionality; and (d) the relative costs and burdens with respect to the proposed forms of production, including the costs of preproduction review, processing, and production.

Illustration i. A party demands that responsive documents, "whether in hard copy or electronic format," be produced. The producing party objects to producing the documents in native electronic format and states that production will be made through PDF or TIFF images on CD-ROMs with load files containing electronically searchable text and selected system and application metadata. The requesting party raises no further objection, and the producing party produces photocopies of the relevant hard copy memoranda, emails and electronic records in a PDF or TIFF format accompanied by a load file containing the searchable text and selected metadata for each item of electronically stored information. This production of electronically stored information satisfies the goals of Principle 12 because the production is in usable form, e.g., electronically searchable and paired with essential metadata.

Illustration ii. Plaintiff claims that he is entitled to a commission on a transaction, based upon an email allegedly sent by the president of defendant corporation agreeing to the commission. Defendant asserts that there is no record of the email being sent in its email system or the logs of its Internet activity, and that the email is not authentic. In these circumstances, it is appropriate to require production of not only the content of the questioned email but also of the email header information and metadata, which can play a crucial role in determining whether the questioned message is authentic.

Illustration iii. Plaintiff alleges that the defendant engaged in a fraud regarding software development. The plaintiff seeks a preliminary order permitting direct access to the hard drives of the software engineers involved and demonstrates that the computer program sold by defendant appears to incorporate plaintiff's source code. In this case, production of the source code in native format may be appropriate, as well as targeted forensic examination of the hard drives concerning the development of the source code. The court should impose such conditions as it deems appropriate to protect legitimate property and privacy interests of the defendant and its employees.

RESOURCES AND AUTHORITIES

Kentucky Speedway, LLC v. NASCAR, Inc., Civ. No. 05-138-WOB, 2006 U.S. Dist. Lexis 92028 (E.D. Ky. Dec. 18, 2006) (court declines to require defendant to supplement production of electronically stored information, relying on a perceived emerging presumption against the production of metadata and citing Sedona Principle 12 (2005 edition)).

In re Priceline.com Inc. Sec. Litig., 233 F.R.D. 88, 91 (D. Conn. 2005) ("Defendants shall produce responsive information contained in stored data files to plaintiffs in TIFF or PDF form with Bates numbering and appropriate confidentiality designations, shall produce searchable metadata databases, and shall maintain the original data itself in native format for the duration of the litigation.").

Compare Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 652 (*"Williams I"*) (D. Kan 2005) ("[W]hen a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to the production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order."), *with Williams v. Sprint/United Mgmt. Co.,* 2006 WL 3691604 (D. Kan. December 12, 2006) (*"Williams II"*) "Defendant raises legitimate concerns about producing the transmittal e-mails with their attachments in their native format, including the whether production in native format would permit the redaction or removal of privileged information. […] Moreover, even assuming that Defendant could produce the transmittal e-mails together with their attachments in native format with the privileged information redacted, Plaintiffs have not sufficiently explained why they need the transmittal e-mails in their native format.").

Comment 12.c. Procedure for requesting and producing metadata under the Federal Rules

Amended Rule 26(f), concerning the conference of parties and planning for discovery, broadly requires parties to address issues related to electronically stored information early in cases where such discovery is at issue. Specifically, Rule 26(f)(3) mandates that the parties meet, confer, and develop a proposed discovery plan that indicates the parties' views and proposals regarding, among other topics, "any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced." To the extent that the parties believe that production of metadata is needed because of either relevance or usability, that should be raised at this conference as it will be a consideration in determining both the need to preserve information in a particular form and the ultimate form or forms of production. By fostering early and ongoing communication between the parties on the issue, the amendments to Rules 26(f) and 34 are designed to lessen the likelihood that disputes over form of production (including metadata issues) will impact the orderly progression of discovery.

Absent an agreement or a court order, Rule 34 establishes a distinct procedure for electronically stored information. Under Rule 34(b), a party serving a request for the production of electronically stored information may, but is not required to, specify the form or forms in which the information should be produced. To the extent that the requesting party seeks a "native" production or some other form of production with accompanying metadata, the revised rule places a burden on the party to make that request explicit. If the requesting party specifies a form or forms of production, the responding party may object to the requested form or forms of production and state the reasons for the objection. Regardless of whether a requesting party fails to state a preferred form of production, or the responding party objects to a requested form, the responding party must state the form or forms in which it intends to produce electronically stored information. In both cases, the producing party should indicate with specificity the forms of production it proposes to use and the requesting party should scrutinize the proposed forms.

Absent party agreement or court order providing otherwise, the responding party must produce electronically stored information in one of two "default forms," the form "in which it is ordinarily maintained," or a form that is "reasonably usable." *See* Comment 12b, *supra*. In addition, absent an agreement or order, a party need not produce the same electronically stored information in more than one form.

Any disputes regarding form or forms of production may be brought before a court for resolution in a variety of ways. The parties may raise any inability to reach agreement at the Rule 16(b) conference so that the court can give initial guidance. The court may place the issue on the calendar for formal resolution, recognizing the possible need for evidence from experts, IT personnel and business users. Parties may also raise the issue by motions – either a motion to compel by the requesting party under Rule 37 or a motion for a protective order by the responding party under Rule 26(c). However, the rules require, and the courts encourage, the parties to attempt to meet and resolve any dispute before filing such motions.

Finally, it is worth noting that a growing tendency in some federal courts is to issue formal local rules or informal guidelines, standards, or "default" case management recommendations addressing electronic production formats. There is much to be gained by such experimentation, but a serious risk exists that these will lead to rigidity and defeat the purpose of the Amended Rules to require parties, not courts, to make the tough choices that fit the particular discovery needs of a case.

RESOURCES AND AUTHORITIES

D. Kan., *Guidelines for Disc. of Electronically Stored Information, available at* http://www.ksd.uscourts.gov/guidelines/electronicdiscoveryguidelines.pdf.

D. Md. Loc. R., *Suggested Protocol for Disc. of Electronically Stored Information, available at* http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf.

N.D. Ohio Civ. App. K, *Default Standard for Discovery of Electronically Stored Information ("E-Discovery"), available at* http://www.ohnd.uscourts.gov/Clerk_s_Office/Local_Rules/AppendixK.pdf.

Comment 12.d. Parties need not produce the same electronically stored information in more than one format

Provided that the forms of production are reasonable, a party should not be required to produce the same information in both hard copy and electronic format, or in both native format and another electronic format. The 2006 Amendments state that production in more than one format is not required, absent an agreement or order. *See* Fed. R. Civ. P. 34(b)(2)(iii). If a court requires production of the same information a second time in a different format because of an unclear or tardy request, the court should consider shifting some or all of the cost of the second production to the requesting party.

RESOURCES AND AUTHORITIES

Williams v. Owens Illinois, Inc., 665 F.2d 918, 933 (9th Cir. 1982) (appellants in employment discrimination case not entitled to computer tapes when they already had access to wage cards containing the same information, even though using the cards "may be more time-consuming, difficult, and expensive").

In re Bristol-Meyers Squibb Sec. Litig., 205 F.R.D. 437, 443 (D.N.J. 2002) (plaintiff not required to pay half of defendant's scanning costs for electronic documents, even though defendant had already produced documents in paper form; although plaintiff was entitled to electronic version, it was already obligated to pay half of photocopying costs for the paper documents and should not be forced to pay for "double-discovery").

Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 652 (D. Kan 2005) ("*Williams I*") ("When a party is ordered to produce electronic document spreadsheets as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to the production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order.").

Exhibit G

Guidelines for Editing Metadata

The District of New Jersey is providing this guideline as a convenience to our efilers, and is unable to provide help-desk support for editing metadata. Efilers are responsible for ensuring that their documents are properly publicized by following the manuals and guides that pertain to the software that they are using.

Table of Contents

Overview

What is metadata?

Metadata is data about data; hidden file information. Metadata becomes a problem when it is accidently released. This document provides guidelines for removing metadata, or at least minimizing its exposure.

There are two types of metadata that are pertinent to us: *revision metadata* and *file description metadata*. *Revision metadata* helps with document editing. The user sees this data when reversing an edit or making other changes by using the **Undo** command. *Revision metadata* remains available until the document is saved using the **Save As**, **Print**, or **Convert (to PDF)** commands, but it is not necessarily removed when using the **Save** command. Documents are most susceptible to inadvertent metadata exposure during this phase.

File description metadata helps manage the file and includes document summary, headers, footers, hyperlinks, OLE object information, and routing slip information. Note: Both types of metadata vary among software applications.

What are the issues associated with metadata?

Metadata can be accidently released when the proper steps are not taken. This problem is predominantly associated with documents in WordPerfect or Microsoft Word that have simply been saved without taking any additional precautions such as removing hidden data, or disabling Track Changes in Microsoft Word and Save Undo/Redo Items in WordPerfect. Most word processing software stores up to the last 10 edits of a document as long as you continue to use **Save** instead of **Save As**.

Most word processing and publishing software provides tools to minimize the risk of inadvertently disclosing *revision metadata*. Alternatively, users should consider sharing documents in PDF format, as this greatly reduces the risk of exposure. Printing documents in PDF format removes *revision metadata,* but not all *file description metadata*. PDF files retain some basic *file description metadata*, such as author, file name, and date, which can be minimized if the proper conversion settings are used (see page 16).

Court users have expressed concerns regarding authorship metadata. When authors create a document using previous versions created by other authors, the original author's name is inherited, leading readers to think it was written by someone else. To avoid this issue, the user should verify and edit the author's name if incorrect through the Properties option (usually found under the File menu of word processing software, see *File Description Metadata* section on page 3). Otherwise, it is suggested to start with a fresh document, and copy and paste text from the existing documents.

There is also concern that some CM/ECF files may contain hidden metadata. The files in CM/ECF are in PDF format, so the risk of *revision metadata* being disclosed is minimal, and *file description metadata* can be minimized, as stated earlier. These final form documents are not where metadata or versioning data has been a problem.

What metadata is associated with a file?

The type of metadata associated with a file depends on the word processing or publishing software. In the Administrative Office of the U.S. Courts and federal courts, Microsoft Word, WordPerfect, and Adobe Acrobat are most commonly used.

- WordPerfect metadata: comments, hidden text, annotations, undo/redo history, document summary data, headers, footers, hyperlinks, OLE object information, and routing slip information.
- Microsoft Word metadata: comments, revision marks from tracked changes, document version information, ink annotations, document properties, (including information from the Summary, Statistics, and custom tabs of the document Properties dialog box), email headers, routing slips, send-for-review information, document server properties, document management policy information, databinding link information for databound fields (last value will be converted to text), user name, template name, and text that is formatted as hidden (a font effect that is available in the font dialog box).
- PDF (Adobe Acrobat) metadata: embedded content; attached files; scripts; hidden layers; embedded search indexes; stored form data; review and comment data; hidden data from previous document saves; obscured text with images; comments hidden from the body of the PDF; unreferenced data, links, actions and JavaScript; and overlapping objects.

Viewing Metadata

The steps for viewing metadata depend on the word processing or publishing software, and may even vary between software versions.

File Description Metadata

Generally, *file description metadata* can be viewed under the Properties option of most software.

WordPerfect

Regardless of the version of WordPerfect, *file description metadata* can be viewed on the Summary tab of the Properties dialog box.

Viewing *file description metadata* in WordPerfect

1. Click **File** on the main menu bar.
2. Select **Properties**.
3. Select the **Summary tab**.
4. Click **OK**.

Microsoft Word

In Microsoft Word, this data can be viewed on several tabs of the Properties dialog box. The steps to access Properties are different for Word 2003, 2007, and 2010.

Viewing *file description metadata* in Microsoft Word 2003

1. Click **File** on the main menu bar.
2. Select **Properties**.

Viewing *file description metadata* in Microsoft Word 2007

1. Click the **Office** button on the main menu bar.
2. Select **Prepare**.
3. Click **Properties**. This will display the Document Information panel across the top of the document. To view the Document Properties dialog box, follow steps 4 and 5.
4. Click **Document Properties** in the Document Information panel.
5. Select **Advanced Properties** (Figure 1).

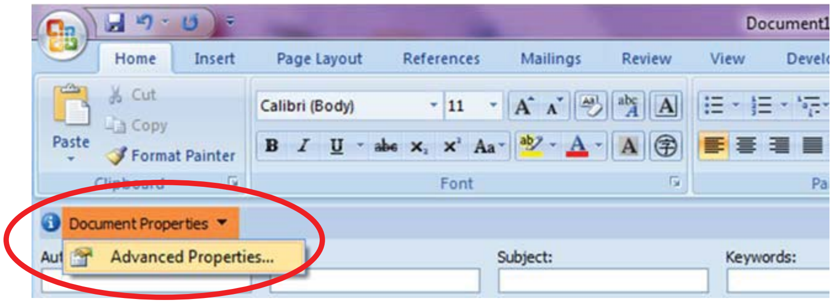
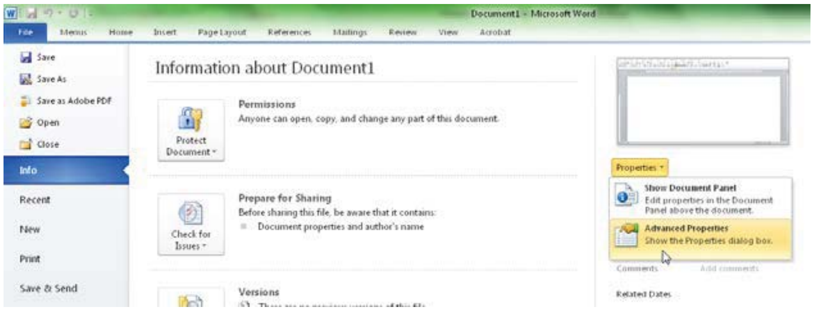


Figure 1: Viewing Document Properties dialog box (Word 2007)

Viewing *file description metadata* in Microsoft Word 2010

1. Click the **File** button on the main menu bar.
2. Select **Info**. General document properties are displayed on the right side of the screen. To view the Document Properties dialog box, follow steps 3 and 4.
3. Click **Properties**.
4. Select **Advanced Properties** (Figure 2).



Information about Document1

Permissions

Anyone can open, copy, and change any part of this document.

Prepare for Sharing

Before sharing this file, be aware that it contains:

- Document properties and author's name

Versions

Edit properties in the Document Panel above the document.

Show the Properties dialog box.

Figure 2: Viewing Document Properties dialog box (Word 2010)

Adobe Acrobat

Regardless of the version of Adobe Acrobat*, file description metadata* can be viewed on the Description tab of the Properties dialog box.

Viewing *file description metadata* in Adobe Acrobat

1. Click **File** on the main menu bar.
2. Select **Properties**.
3. Select the **Description** tab (default). To view additional *file description metadata*, click the **Additional Metadata** button.
4. Click **OK** on Additional Metadata dialog box, if opened.
5. Click **OK** on Properties dialog box.

Revision Metadata

The methods of viewing of *revision metadata* vary between word processing and publishing software, as well as between versions.

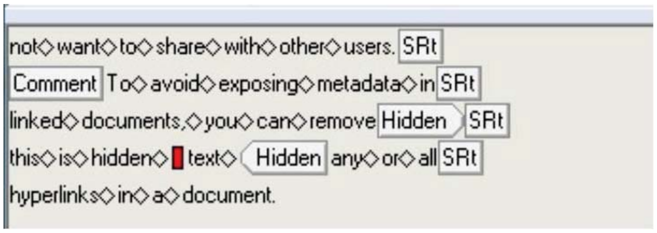
WordPerfect

The file format of WordPerfect makes it easy to view *revision metadata* by using the reveal codes feature (Figure 3).

Viewing *revision metadata* in WordPerfect

1. Click **View** on the main menu bar.
2. Select **Reveal Codes**.

OR
Type **Alt + F3**.



not◇want◇to◇share◇with◇other◇users. SRt
Comment To◇avoid◇exposing◇metadata◇in SRt
linked◇documents,◇you◇can◇remove Hidden SRt
this◇is◇hidden◇▮ text◇ Hidden any◇or◇all SRt
hyperlinks◇in◇a◇document.

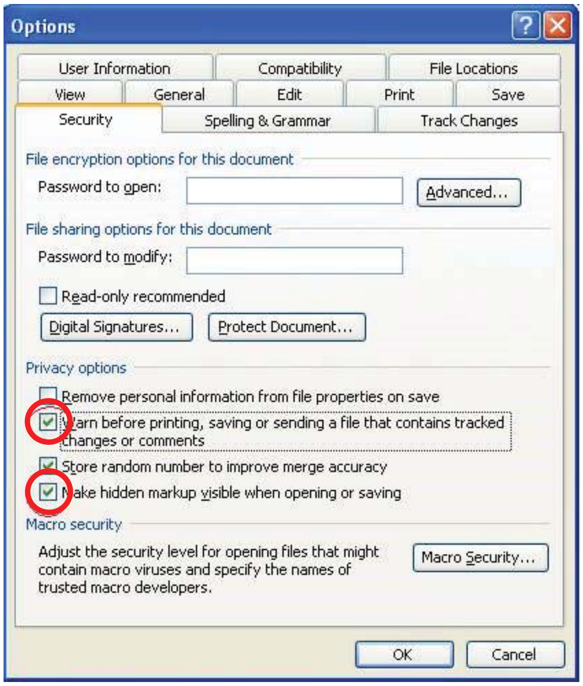
Figure 3: WordPerfect's Reveal Codes showing document metadata (comments and hidden text)

Microsoft Word

In Microsoft Word, most *revision metadata* can be accessed by having the proper security settings. The steps needed to set proper security settings vary for Word 2003, 2007, and 2010.

Viewing *revision metadata* in Microsoft Word 2003

1. Click **Tools** on the main menu bar.
2. Select **Options**.
3. Select the **Security** tab in the Options dialog box.
4. Check **Warn before printing, saving or sending a file that contains tracked changes or comments** and **Make hidden markup visible when opening or saving**, if they are unchecked (Figure 4).
5. Click **OK**.



File encryption options for this document

Password to open:

File sharing options for this document

Password to modify:

☐ Read-only recommended

Privacy options

☐ Remove personal information from file properties on save

☑ Warn before printing, saving or sending a file that contains tracked changes or comments

☑ Store random number to improve merge accuracy

☑ Make hidden markup visible when opening or saving

Macro security

Adjust the security level for opening files that might contain macro viruses and specify the names of trusted macro developers.

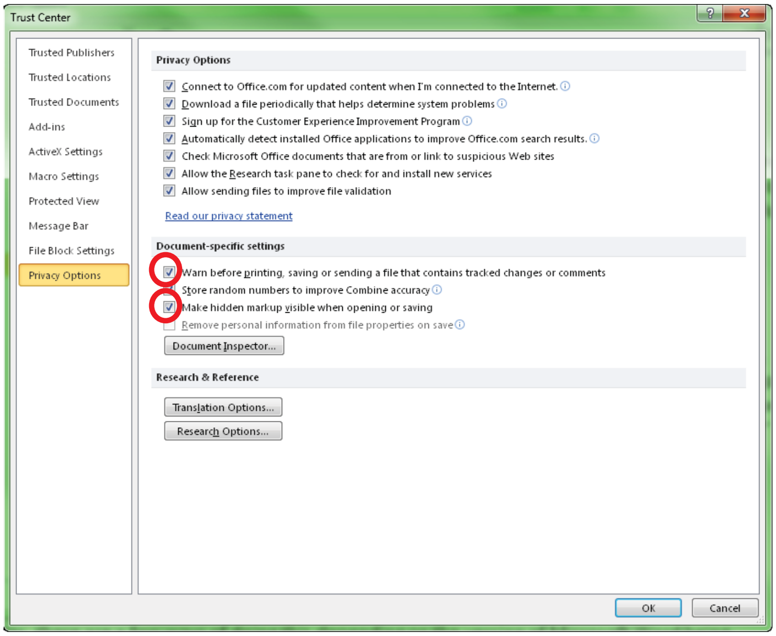
Figure 4: Security Settings for displaying revision metadata (Word 2003)

Viewing *revision metadata* in Microsoft Word 2007

1. Click the **Office** button on the main menu bar.
2. Click **Word Options** at the bottom right of the menu; this will display the Word Options dialog box.
3. Select the **Trust Center** option on the left pane.
4. Click the **Trust Center Settings** button; this will open the Trust Center dialog box.
5. Select **Privacy Options** in the left pane.
6. Check **Warn before printing, saving or sending a file that contains tracked changes or comments** and **Make hidden markup visible when opening or saving**, if they are unchecked (Figure 5).
7. Click **OK**.

Viewing *revision metadata* in Microsoft Word 2010

1. Click the **File** button on the main menu bar.
2. Select **Options**; this will display the Word Options dialog box.
3. Select the **Trust Center** option on the left pane.
4. Click the **Trust Center Settings** button; this will open the Trust Center dialog box.
5. Select **Privacy Options** in the left pane.
6. Check **Warn before printing, saving or sending a file that contains tracked changes or comments** and **Make hidden markup visible when opening or saving**, if they are unchecked (Figure 5).
7. Click **OK**.



Privacy Options

☑ Connect to Office.com for updated content when I'm connected to the Internet.
☑ Download a file periodically that helps determine system problems
☑ Sign up for the Customer Experience Improvement Program
☑ Automatically detect installed Office applications to improve Office.com search results.
☑ Check Microsoft Office documents that are from or link to suspicious Web sites
☑ Allow the Research task pane to check for and install new services
☑ Allow sending files to improve file validation

Read our privacy statement

Document-specific settings

☑ Warn before printing, saving or sending a file that contains tracked changes or comments
☑ Store random numbers to improve Combine accuracy
☑ Make hidden markup visible when opening or saving
☐ Remove personal information from file properties on save

Research & Reference

Figure 5: Privacy Options for displaying revision metadata (Word 2010)

Adobe Acrobat

The Examine Document tool in Adobe Acrobat 8 and 9 scans the PDF and identifies potentially hidden information: metadata, comments, bookmarks, file attachments, and even “hidden text” (text hidden by another object or white text on white background). In Adobe Acrobat X and Adobe Acrobat X Pro, the tool is now called Remove Hidden Information.

Please note that “hidden text” is not only an issue of inadvertently releasing metadata but also of improper redaction practices.[1]

Viewing *revision metadata* in Adobe Acrobat 9

1. Click **Document** on the main menu bar.
2. Click **Examine Document**; this will display results on the Examine Document pane on the left side of the screen.
3. Click the **expand** icon on the Examine Document pane so that all information is displayed on the results list. To view metadata, click the **Show preview** option (Figure 6).
4. Close the Examine Document pane.

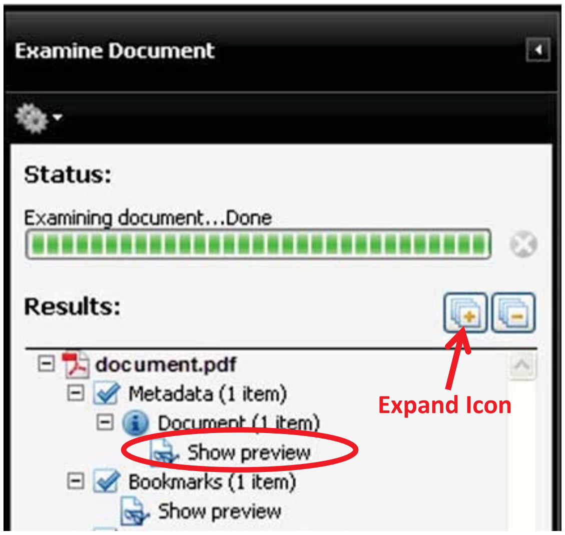
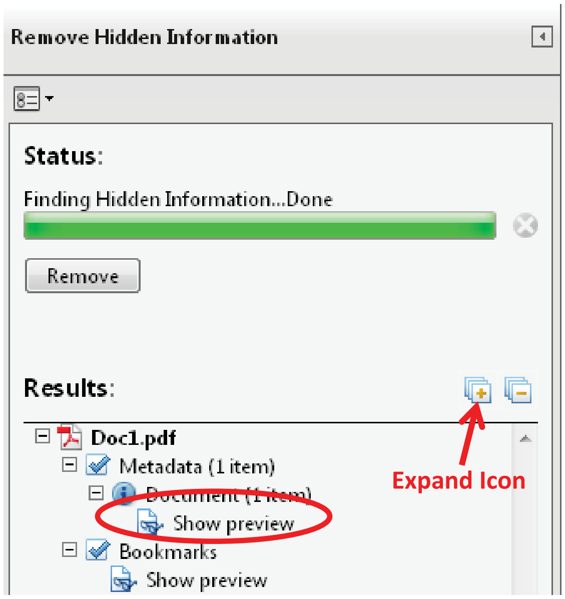


Figure 6: Examine Document (Acrobat 9)

[1] Additional information regarding this issue as it relates to the courts can be found on the Utah District Court blog entry “Redaction Warnings!” published online at http://utd-cmecf.blogspot.com/search?q=metadata.

Viewing *revision metadata* in Adobe Acrobat X and Adobe Acrobat X Pro

1. Click **Tools** on the top right of the screen.
2. Select **Protection**.
3. Select **Remove Hidden Information**; this will open the Remove Hidden Information pane on the left side of the screen.
4. Click the **expand** icon on the Remove Hidden Information pane so that all information is displayed on the results list. To view metadata, click the **Show preview** option (Figure 7).
5. Close the Remove Hidden Information pane.



Status:

Finding Hidden Information...Done

Figure 7: Remove Hidden Information Pane (Acrobat X Pro)

Removing Metadata

Depending on the software, there are several methods to remove metadata. In most word processing applications, **Save As** creates a clean file, removing *revision metadata* (results may vary depending on version). You can also use the PDF printer (Distiller) to create a clean file. In addition, there are metadata removal tools available through word processing and publishing software or third parties.

WordPerfect

Steps and tools for removing metadata in WordPerfect depend on the software version.

Removing metadata in WordPerfect 12 or earlier

You will need to manually remove the *revision* and *file description* metadata. The link below provides instructions on how to manually clean up metadata.

Minimizing metadata in WordPerfect 12 document [2]

Removing metadata in WordPerfect X3 or newer

1. Click **File** on the main menu bar.
2. Select **Save Without Metadata**.
3. Check the metadata that you wish to remove.
4. Click **Save**.

The link below provides additional information on using the Save Without Metadata option.

Saving documents without metadata[3]

Note, if you are using WordPerfect X3 or newer and do not see the Save Without Metadata option, you can add it to your menu bar.

Adding the Save Without Metadata option to WordPerfect X5

1. Click **Tools** on the main menu bar OR right-click on the main menu bar and select Settings. (If you do this, skip to number 4.)
2. Select **Settings** from the dropdown list.
3. Click **Customize** on the Settings dialog box.
4. Select the **Menus** tab on the Customize Settings dialog box.
5. Click the **Edit** button.
6. Under Features, select **Save Without Metadata** and drag it to **File** on the main menu bar (Figure 8). Or click **Add Menu Item**, which adds the option directly to the main menu bar.
7. Click **OK** in the Menu Editor dialog box.
8. Click **Close** in the Customize Settings dialog box.
9. Click **Close** in the Settings dialog box, if it is open.

[2] http://www.corel.com/content/pdf/wpo12/Minimizing_Metadata_In_WordPerfect12.pdf
[3] http://www.corel.com/corel/pages/index.jsp?pgid=800411&item=resource&listid=1600090

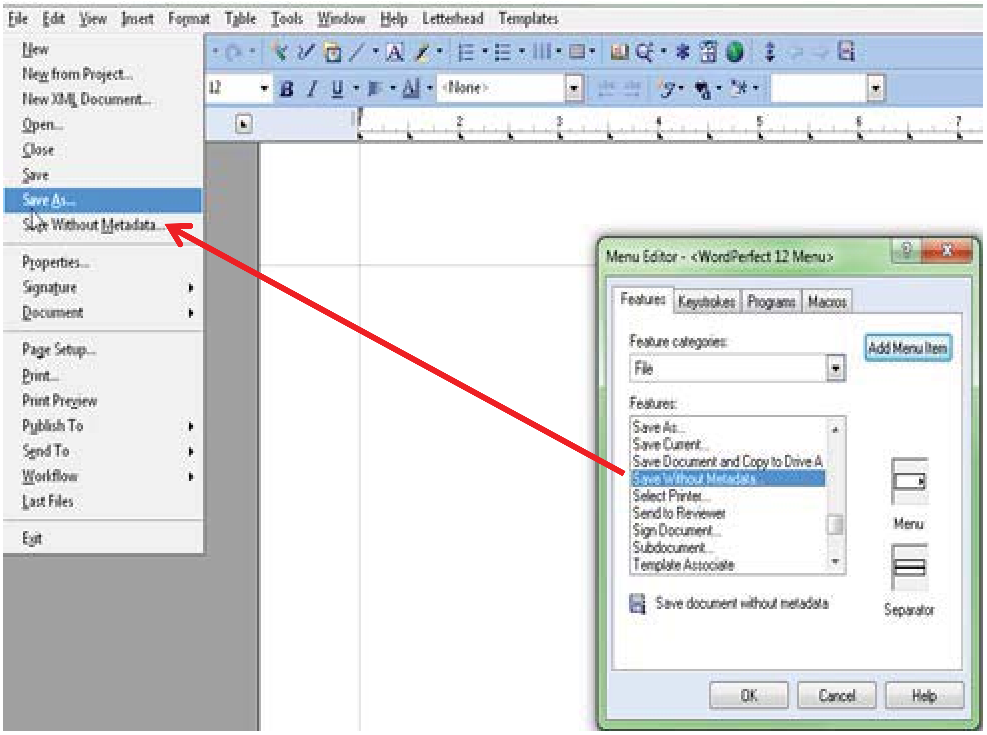


Figure 8: Adding Save Without Metadata to File menu

Microsoft Word

In Word 2003, you must remove metadata manually. However, in Word 2007 or 2010, the Document Inspector feature (Figure 9) allows you to select the metadata you want to remove.

Removing metadata in Word 2003

The link below provides instructions on how to manually clean up *revision* and *file description* metadata.

How to minimize metadata in Word 2003[4]

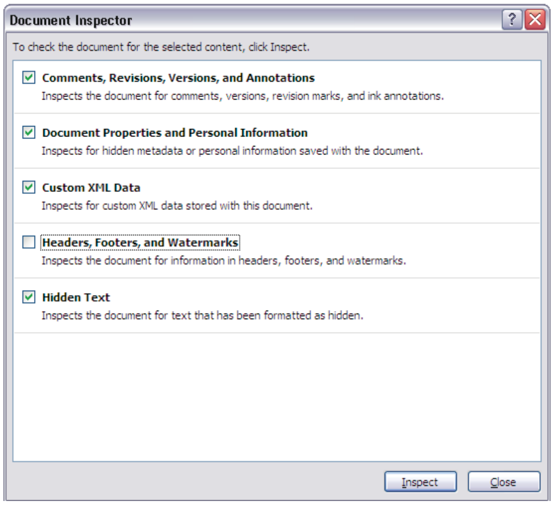
[4] http://support.microsoft.com/kb/825576

Removing metadata in Microsoft Word 2007

1. Click the **Office** button on the main menu bar.
2. Select **Prepare**.
3. Click **Inspect Document**; this will display Document Inspector dialog box (Figure 9).
4. Check the content you want to inspect for.
5. Click **Inspect**.
6. Click the **Remove All** button next to the content you would like to remove.
7. Click **Close**. If you would like to reinspect the document to verify content was removed, click **Reinspect**; this will take you back to step 4.

Additional information may be found using the following link:

Remove hidden data and personal information from Office documents[5]



To check the document for the selected content, click Inspect.

☑ **Comments, Revisions, Versions, and Annotations**
Inspects the document for comments, versions, revision marks, and ink annotations.

☑ **Document Properties and Personal Information**
Inspects for hidden metadata or personal information saved with the document.

☑ **Custom XML Data**
Inspects for custom XML data stored with this document.

☐ **Headers, Footers, and Watermarks**
Inspects the document for information in headers, footers, and watermarks.

☑ **Hidden Text**
Inspects the document for text that has been formatted as hidden.

Figure 9: Document Inspector dialog box for reviewing metadata (Word 2007)

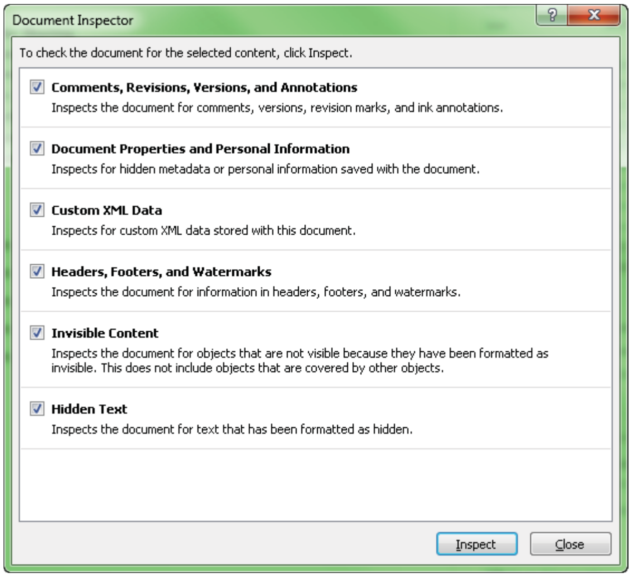
[5] http://office.microsoft.com/en-us/excel-help/remove-hidden-data-and-personal-information-from-office-documents-HA010037593.aspx

Removing metadata in Microsoft Word 2010

1. Click the **File** button on the main menu bar.
2. Select **Info**.
3. Click **Check for Issues**.
4. Select **Inspect Document**; this will display Document Inspector dialog box (Figure 10).
5. Check the content you want to inspect for.
6. Click **Inspect**.
7. Click the **Remove All button** next to the content you would like to remove.
8. Click **Close**. If you would like to reinspect the document to verify that content was removed, you can do so by clicking **Reinspect**; this will take you back to step 5.

Additional information may be found using the following link:

Remove hidden data and personal information by inspecting documents Word 2010[6]



Document Inspector

To check the document for the selected content, click Inspect.

☑ **Comments, Revisions, Versions, and Annotations**
Inspects the document for comments, versions, revision marks, and ink annotations.

☑ **Document Properties and Personal Information**
Inspects for hidden metadata or personal information saved with the document.

☑ **Custom XML Data**
Inspects for custom XML data stored with this document.

☑ **Headers, Footers, and Watermarks**
Inspects the document for information in headers, footers, and watermarks.

☑ **Invisible Content**
Inspects the document for objects that are not visible because they have been formatted as invisible. This does not include objects that are covered by other objects.

☑ **Hidden Text**
Inspects the document for text that has been formatted as hidden.

Figure 10: Document Inspector dialog box for reviewing metadata (Word 2010)

Adobe Acrobat

As mentioned previously, Adobe Acrobat 8 and 9 provide the Examine Document function, which removes metadata. This feature scans the document and allows you to remove any hidden information with a single click. In Adobe Acrobat X and Adobe Acrobat X Pro, the tool is called Remove Hidden Information. Adobe Acrobat X Pro's Sanitize Document option strips the document by converting it into an image; however, this also removes the ability to perform text searches, so the Sanitize Document option is not recommended.

[6] http://office.microsoft.com/en-us/word-help/remove-hidden-data-and-personal-information-by-inspecting-documents-HA010354329.aspx

Removing metadata in Adobe Acrobat 9

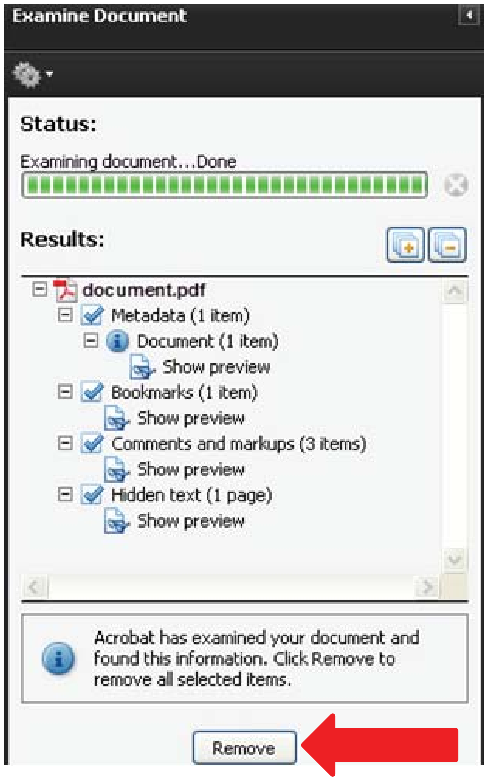
1. Click **Document** on the main menu bar.
2. Click **Examine Document**; this will display results on the left-side navigation pane.
3. Uncheck the content or metadata that you do not want to remove (Figure 11).
4. Click **Remove**.
5. Click **OK**.

To configure Adobe Acrobat to remind you to remove metadata when closing, follow the steps below:

1. Click **Edit** on the main menu bar.
2. Click on **Preferences**.
3. Select **Documents** from the Categories list on the left pane.
4. Check **Examine document when closing document**.
5. Click **OK**.

Additional information may be found using the following link:

Examine a PDF for hidden content – Adobe Acrobat 9 Standard Help[7]



Status:

Examining document...Done

Results:

- document.pdf
  - ☑ Metadata (1 item)
    - Document (1 item)
      - Show preview
  - ☑ Bookmarks (1 item)
    - Show preview
  - ☑ Comments and markups (3 items)
    - Show preview
  - ☑ Hidden text (1 page)
    - Show preview

Acrobat has examined your document and found this information. Click Remove to remove all selected items.

Figure 11: Examine Document (Acrobat 9)

[7] http://help.adobe.com/archive/en_US/acrobat/9/standard/acrobat_standard_9.0_help.pdf#page=242

Removing metadata in Adobe Acrobat X and Adobe Acrobat X Pro

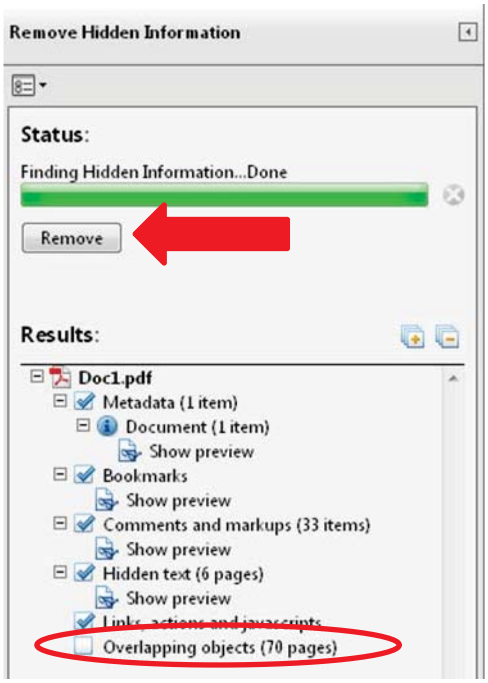
1. Click **Tools** on the top-right of the screen.
2. Select **Protection**.
3. Select **Remove Hidden Information**; this will open the Remove Hidden Information pane on the left side of the screen.
4. Uncheck the content or metadata that you do not want to remove. This allows you to sanitize the document without removing the text search capability. In order to preserve text search capabilities, you should uncheck overlapping objects (Figure 12).
5. Click **Remove**.
6. Click **OK**.

To configure Adobe Acrobat to remind you to remove metadata when closing , follow the steps below:

1. Click **Edit** on the main menu bar.
2. Click on **Preferences**.
3. Select **Documents** from the Categories list on the left pane.
4. Check **Remove Hidden Information when closing document**.
5. Click **OK**.

Additional information may be found using the following link:

Remove Sensitive Content (Metadata and Redaction) – Adobe Acrobat X Pro Help[8]



Remove Hidden Information

Status:

Finding Hidden Information...Done

Results:

Doc1.pdf
- ☑ Metadata (1 item)
  - Document (1 item)
    - Show preview
- ☑ Bookmarks
  - Show preview
- ☑ Comments and markups (33 items)
  - Show preview
- ☑ Hidden text (6 pages)
  - Show preview
- ☑ Links, actions and javascripts
- □ Overlapping objects (70 pages)

Figure 12: Remove Hidden Information Pane (Acrobat X Pro)

[8] http://help.adobe.com/en_US/acrobat/X/pro/using/WS4E397D8A-B438-4b93-BB5F-E3161811C9C0.w.html

Adobe Acrobat also offers ways to automate metadata scrubbing. We do not recommend any method in particular, as this depends on user need. Scrubbing can be a backend solution performed by the IT staff (see references listed below). Additionally, Adobe Acrobat X Pro provides a new feature (Action Wizard) that can be used to automate the metadata removal. [9]

Information on how to automate metadata scrubbing:

Scrubbing Metadata – Practice and Policy[10]

Find and Remove PDF Metadata[11]

Converting to PDF

Converting documents from word processing to PDF format scrubs their *revision metadata*. Prior to converting or printing to PDF, the document should be properly scrubbed using tools provided by the authoring word processor or other tools available. In addition, you should verify that the proper conversion/print settings are configured. Some of the inherited *file description metadata* includes document author, document title, document keyword, etc.

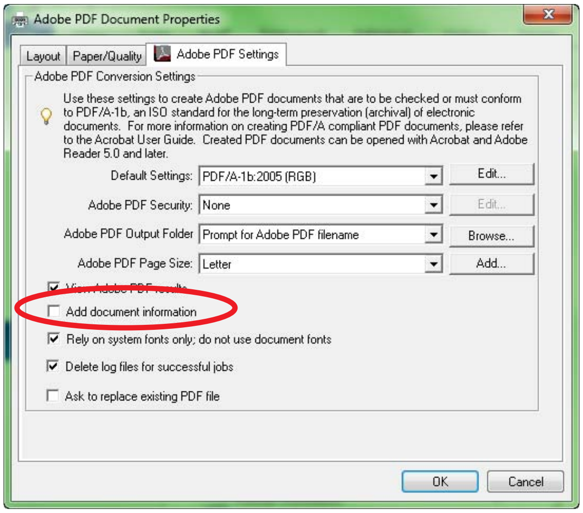
Setting Adobe PDF Conversion Settings (Print to PDF – Microsoft Word 2010/WordPerfect)

1. Click **File** on the main menu bar.
2. Select **Print**.
3. Select **Adobe PDF** as printer on the Print dialog box.
4. Click **Printer Properties** (Word) or **Properties** (WordPerfect); this will open the Adobe PDF Document Properties dialog box.
5. Uncheck the **Add document information** checkbox (Figure 13).
6. Click **OK**.

[9] The following link provides additional guidance for Action Wizard: http://tv.adobe.com/watch/acrobat-x/how-to-create-actions/.

[10] http://blogs.adobe.com/acrobat/scrubbing-metadata-practice-and-policy/

[11] http://www.microsystems.com/resources/wordtips/wordtip003.php



Adobe PDF Document Properties

Adobe PDF Conversion Settings

Use these settings to create Adobe PDF documents that are to be checked or must conform to PDF/A-1b, an ISO standard for the long-term preservation (archival) of electronic documents. For more information on creating PDF/A compliant PDF documents, please refer to the Acrobat User Guide. Created PDF documents can be opened with Acrobat and Adobe Reader 5.0 and later.

Default Settings: PDF/A-1b:2005 (RGB)

Adobe PDF Security: None

Adobe PDF Output Folder: Prompt for Adobe PDF filename

Adobe PDF Page Size: Letter

☑ View Adobe PDF results

□ Add document information

☑ Rely on system fonts only; do not use document fonts

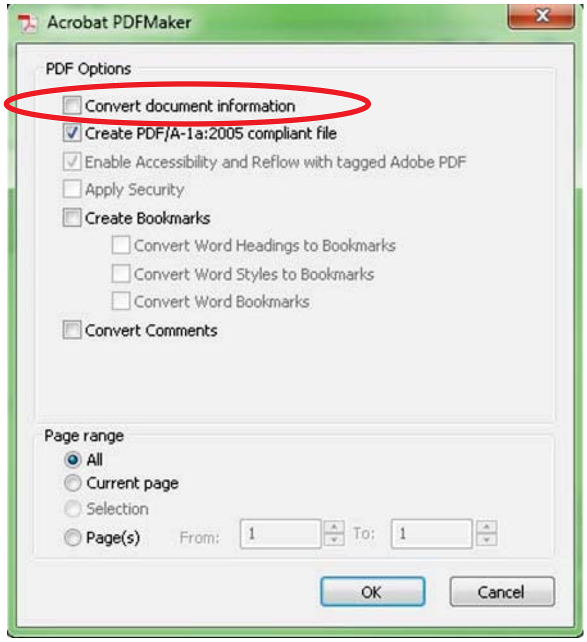
☑ Delete log files for successful jobs

□ Ask to replace existing PDF file

Figure 13: PDF Settings when printing to PDF file

Setting Adobe PDF Conversion Settings (Save as Adobe PDF – Microsoft Word 2010)

1. Click **File** on the main menu bar.
2. Select **Save as Adobe PDF**; this will open the Save Adobe PDF File As dialog box.
3. Click the **Options** button; this will open the Acrobat PDFMaker dialog box.
4. Uncheck the **Convert document information** checkbox (Figure 14).
5. Click **OK**.
6. Click **Save**.



Acrobat PDFMaker

PDF Options

□ Convert document information

☑ Create PDF/A-1a:2005 compliant file

☑ Enable Accessibility and Reflow with tagged Adobe PDF

□ Apply Security

□ Create Bookmarks

□ Convert Word Headings to Bookmarks

□ Convert Word Styles to Bookmarks

□ Convert Word Bookmarks

□ Convert Comments

Page range

● All

○ Current page

○ Selection

○ Page(s) From: 1 To: 1

Figure 14: Adobe PDFMaker dialog box (Word 2010)

Exhibit H

I CAN TELL WHEN YOU'RE TELLING LIES: ETHICS AND EMBEDDED CONFIDENTIAL INFORMATION

David Hricik[*]

I. INTRODUCTION

The risk of inadvertently transmitting what a lawyer knows is confidential information to an opposing or third party has always existed. Not too long ago, the primary risk was that a letter intended for a client would instead be mailed or faxed to opposing counsel.[1] For example, a lawyer might have made handwritten comments on a contract proposal drafted by the other side, and, though intending to forward the document to the client for review, may have inadvertently mailed or faxed it to opposing counsel.

The digital age has increased the opportunity for and changed the means by which misdirection occurs, but in substance the circumstances leading to misdirection remain the same. Instead of misaddressing envelopes, today lawyers and their staff may inadvertently send e-mail intended for a client to opposing counsel or a third party or accidentally forward to opposing counsel an e-mail received from a client.[2]

Despite these changes in form, the ethical principles that apply to these typical forms of digital misdirection are no different than those that apply in the analog world. The lawyer who inadvertently discloses a client's confidences can violate ethical duties,[3] and at the same time a lawyer who re-

[*] Professor Hricik is an Associate Professor of Law at Mercer University School of Law in Macon, Georgia. He has written extensively on the ethical issues arising from high technology. *See, e.g.*, David Hricik, *To Whom it May Concern: Using Disclaimers to Avoid Disqualification by Receipt of Unsolicited E-mail from Prospective Clients*, 16 PROF. LAW., Fall 2005, at 1; David Hricik & Robert Jueneman, *The Transmission and Receipt of Invisible Confidential Information*, 15 PROF. LAW., Spring 2004 at 18; David Hricik, *The Use of Website Disclaimers Regarding the Obligation of Confidentiality for U.S. Law Firms*, 4 WORLD INTERNET L. REP., Sep. 2004, at 29; David Hricik, *Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-mail*, 11 GEO. J. LEGAL ETHICS 459 (1998). The title is from "I Can Tell When You're Telling Lies" from the compact disc by John Wesley Harding, THE NAME ABOVE THE TITLE (Sire/Reprise 1991). I would like to thank my Research Assistant, Amy Falkingham, for her invaluable assistance on this Article.

[1] *See generally* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992) (describing such scenarios).

[2] *See generally* Steven L. Nelson & Jane C. Schlicht, *Upholding the Sanctity of the Attorney-Client Privilege*, 77 WIS. LAW., Dec. 2004, at 8 (describing hypotheticals); Emily Eichenhorn, *Risks & Rewards: Resisting the Inclination to Abdicate to Technology*, 63 OR. ST. BAR BULL., Apr. 2003, at 40.

[3] *See generally* MODEL RULES OF PROF'L CONDUCT R. 1.6 (2004).

ceives privileged information not intended for him may be ethically required to return the information unread, or take other steps.[4]

The focus of this Article is a slightly more interesting and as yet largely unanalyzed form of misdirection: the intentional transmission of a computer file that carries with it "invisible"[5] confidential information. The presence of this "invisible" information presents new twists on this old ethical problem, and the invisible information can be as important—if not more so—as the visible content of the file. The invisible information that accompanies some files "can reveal a cache of information, including the names of everyone who has worked on or seen a specific document, text and comments that have been deleted and different drafts of the document."[6]

The question of lawyer's responsibilities concerning the transmission and receipt of this information presents issues distinct from both the traditional misdirected letter and its modern counterpart, the misdirected e-mail, from the perspective of both the sender and recipient. This Article addresses two distinct issues that metadata and similar forms of electronic data present. (Collectively, metadata and similar forms of data are referred to as "embedded data.").

First, it analyzes whether lawyers have an obligation to be aware of embedded data and, as a consequence, to remove it from documents where it is ethically necessary and proper to do so. Did Macrosoft's lawyers, for example, violate duties to their client by unknowingly sending embedded data along with the text of the contract to opposing counsel? If there is such an obligation, what must lawyers do to comply with it?

Second, if a lawyer receives a file that contains embedded data that reveals confidential or privileged information of an opposing party, do the same obligations apply as when a lawyer receives a document in a misaddressed envelope?[7] For example, did the lawyer who examined Macrosoft's internal commentary about the contract's terms violate any ethical obligations? If so, what does a lawyer who receives an electronic file do?

This Article addresses these issues[8] but begins with an overview of the various common forms of embedded data before turning to the ethical issues that it creates.

[4] *See* Formal Op. 92-368, *supra* note 1.

[5] *See infra* note 6 and accompanying text (The information is not really invisible. It can be viewed, but only if certain steps are taken. Those steps, however, do not require special software; the "invisible" information may be examined by using the program that created the file). In addition, programs specifically designed to view embedded data also exist.

[6] Jason Krause, *Hidden Agendas: Unlocking Invisible Electronic Codes Can Reveal Deleted Text, Revisions,* 90 A.B.A. J., July 2004, at 26.

[7] *See infra* notes 71-98 and accompanying text.

[8] Embedded data presents a third issue of competency for litigators during discovery in disputes where there exist relevant electronically-created documents. Just as the fax band may show that the opposing party is lying when he claims not to have received a document, so too embedded data may be highly relevant to a party's claim or defense in litigation. Therefore, is there an ethical obligation to seek out and discover the original files of critical documents in a case, so as to examine the embedded data for pertinent information? If, for example, a dispute arose over that contract with Macrosoft, do the litigators have an ethical obligation to seek out discovery of the actual electronic files, since the embedded

II. WHAT IS EMBEDDED DATA?

A. Overview of Embedded Data and Its Purposes

There are two somewhat similar forms of information that accompany electronic files: metadata and other information that is stored, and thus transmitted along, with electronic files.[9]

First, metadata is "data about data."[10] Although it sounds quite modern, one form of metadata is no doubt familiar to every lawyer: the fax band on a document received by facsimile. Typically, it shows the time and date the document was received, the number from which the fax originated, and the number of pages sent.[11] A fax band is metadata, since it is data about data. The factual data it contains can be used in various ways. For example, it can be used to show that a party who claims it did not receive a document did receive it on a certain date.

Metadata pervades the digital world in which we live. Electronic files created by many common programs create metadata—hidden fax bands, and more—that is generally saved along with the visible text of the document. Oversimplifying it, "invisible fax bands" accompany files created by many modern computer programs. Metadata is embedded with the file and goes anywhere the file goes unless it is removed by the file's creator prior to transmission. Any time the file is transmitted to another person, the fax bands go along with the file. But, rather than simply detailing the time and date the file was prepared, as would a true fax band, metadata often reveals much more.[12]

data may reveal more than the printed text alone? If so, how do they go about satisfying that obligation? Those issues have been repeatedly addressed in the literature. *See generally* Bahar Shariati, *Zubulake v. UBS Warburg: Evidence that the Federal Rules of Civil Procedure Provide the Means for Determining the Cost Allocation in Electronic Discovery Disputes?*, 49 VILL. L. REV. 393 (2004); Sedona Conference Working Group on Electronic Document Retention and Production, *The (2004) Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 5 SEDONA CONF. J. 151 (2004); Whitney Adams & Jeffery Jacobs, *Ghost in the Machine: Legal Developments and Practical Advice in an Age of Electronic Discovery*, 22 ACC DOCKET 48 (2004) (noting that protective orders in civil litigation are beginning to specifically address the obligations of counsel pertaining to embedded data). *See, e.g.*, Jicarilla Apache Nation v. U.S., 60 Fed. Cl. 413 (Cl. Ct. 2004); *In re* Verisign, Inc. Sec. Litig., No. C 02-02270 JW, 2004 WL 2445243, at *1 (N.D. Cal. Mar. 10, 2004).

Those issues are distinct from the issues raised here, which presume the absence of anticipated or actual litigation. Where litigation becomes anticipated, duties to preserve embedded data and to avoid spoliation may arise. *See* Gene Klimov & Suzan Flamm, Data Preservation Protocols Post Zubulake, SK071 ALI-ABA 179 (2005).

[9] Often the two types are lumped into "metadata." *E.g.*, James Q. Walker, *Ethics and Electronic Media*, 716 PLI/LIT 313, 328 (2004); Carole Levitt & Mark Rosch, *Making Metadata Control Part of a Firm's Risk Management*, 28 L.A. LAW. 40, 40 (2005). I prefer to separate out what is truly metadata—data reflecting when or who edited a document, for example—from other information that can be embedded in data files, such as prior revisions and undo histories. Treating the two as the same risks conflating the issue of whether confidentiality or privilege is likely to be conveyed by the transmission of files with embedded data. *See infra* notes 10-16 and accompanying text.

[10] Gerald J. Hoenig, *Technology Property*, 18 PROB. & PROP, Sept./Oct. 2004, at 51.

[11] *See infra* note 12 and accompanying text for an example.

[12] *See infra* notes 19-37 and accompanying text.

Electronic files are often accompanied by a similar, but distinct, form of information. In addition to metadata, many software programs permit authors to "[t]rack [c]hanges"[13] to the text, to save "multiple undoes" in case the author later decides to "undo" revisions made previously, and to even overlay hidden comments into the text.[14] This other information is also embedded with the file and accompanies the file unless removed prior to transmission.

An ostensibly true story demonstrates the potential risks of exchanging files with embedded data.[15] Recently, a lawyer approached me after I had given a presentation about metadata and told me the following story. He had been negotiating a contract against a well-known software maker, whom we'll call "Macrosoft." During negotiations, the lawyers for each side used Microsoft Word to propose revisions to the contract, using its "track changes" feature to allow the recipient to see the specific changes each lawyer had made. They would e-mail the file with embedded data back and forth to each other between rounds of revisions. When the lawyer received one draft of the contract from Macrosoft's lawyers, he made a few mouse clicks and was easily able to reveal—without using anything but Microsoft Word—various "hidden" embedded data. As a result, he was able to read all of the internal comments that the sending lawyer had received from Macrosoft's business people concerning the terms of the contract, negotiating positions, and bottom-lines.

The receiving lawyer learned Macrosoft's critical bargaining information by clicking a button. He was able to see not only metadata showing who had revised the document, but also internal private comments that lawyers and business people on the other side had made. Thus, had a Macrosoft lawyer insisted during negotiations that the noncompetition clause was extremely important to Macrosoft, the lawyer I spoke to could use the internal comments where Macrosoft personnel had discussed the issue amongst themselves to tell if this were true, or if it was simply a negotiating ruse. He could tell when they were telling lies.

With that background, it is important to clarify the purpose of embedded data—it is there for a reason—before turning to specific examples of where embedded data can be found in the programs commonly used by lawyers today.[16]

[13] Levin & Rosch, *supra* note 9, at 41.

[14] *See infra* notes 19-37 and accompanying text.

[15] Another author posited this example:

> Imagine the embarrassment, the lost negotiation leverage, and the potential liability of a lawyer for a mortgage lender who, via metadata, discloses to the other side that the client does not want the closing to be delayed to negotiate the exclusions from the nonrecourse provision and that the client is willing to delete two of the exclusions if the borrower simply asks for the deletions.

Gerald J. Hoenig, *supra* note 10, at 51.

[16] *See generally* Levitt & Rosch, *supra* note 9, at 40 (describing embedded data created by Word and WordPerfect).

Embedded data is not created to cause the unintended exchange of confidential information. Although the form taken by embedded data varies among programs, the primary function of embedded data is utilitarian: it is designed to help users of software revise, organize, and access electronically-created files.[17] Typical metadata includes, for example, the person who authored the document and its location (drive, folder). In addition, other embedded data can include records of past revisions. A secretary can, as a result, examine the changes that have been made to a file and compare them visually to any hand-written revisions to ensure that they have, in fact, been made. Thus, embedded data is useful.[18]

B. Specific Examples of Metadata

This section provides some simple examples of embedded data to illustrate the kind and quality of information that these files can convey. Note that some of the particular illustrations and examples in each section will vary depending on the version of the software used.

1. Microsoft Word

In my experience, lawyers commonly use Microsoft Word and commonly e-mail documents created by Microsoft Word to clients, third parties, and opposing counsel. It has rightly been called the "ubiquitous" software program.[19] Embedded data is, unfortunately, ubiquitous in Word.

Metadata can be found by looking in different menu items in Microsoft Word.[20] A key location is in the "Properties" item, located in the "File" menu. The "Properties" for a particular document can reveal the author, creation dates, and other information. For example, this particular article (as of about halfway through the writing process), contains the information under File/Properties as shown in Figure 1.

[17] *See generally* Brian D. Zall, *Metadata: Hidden Information in Microsoft Word Documents and Its Ethical Implications*, 33 COLO. LAW., Oct. 2004, at 53.

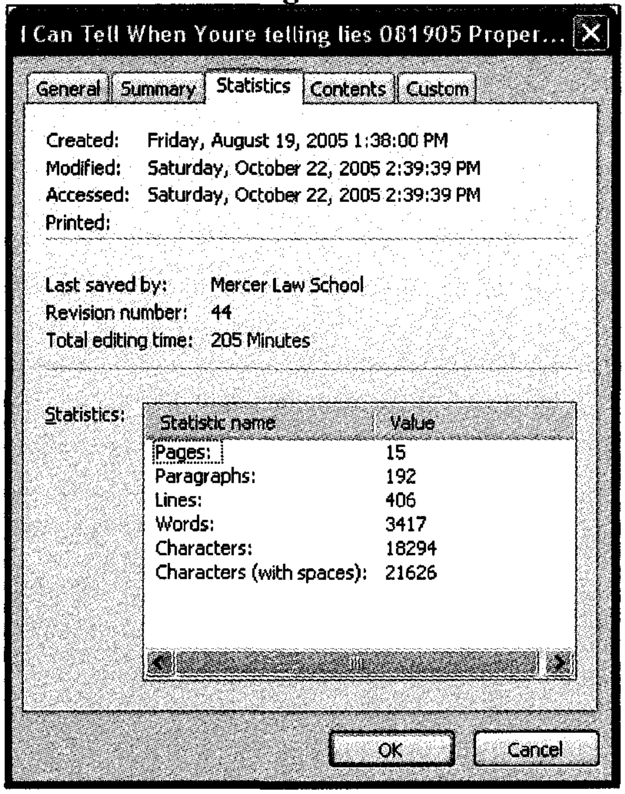
[18] *See generally* Hoenig, *supra* note 10. "Word has built-in tools to facilitate collaboration among members of a team." *Id.* at 51.

[19] Andrew Beckerman-Rodau, *Ethical Risks from the Use of Technology*, 31 RUTGERS COMPUTER & TECH. L.J. 1, 32 (2004); *see also* Zall, *supra* note 17, at 53-54 (describing legal profession's adoption of Microsoft Word).

[20] Interestingly, most metadata is stored in the last space of a Word document. If, for example, you copy all of a Word document except its last space (which will appear to be blank) and then paste that material into a new Word document, the prior metadata will not follow along. For a more technical discussion of how metadata is embedded in a Word document, *see* Zall, *supra* note 17, at 54.

The metadata on just that single screen[21] reveals the fact that I began to write this Article in August, and was still working on it in October, 2005. It also reveals that, as of the time I viewed that screen, it was the 44th revision (meaning I had opened and closed this document 44 times) and I had edited it for 205 minutes.[22] If this document had been transmitted to a client, the client could have some insight into whether I had worked on it for as long as I said in my fee statement. If it were a report I had prepared as an expert witness, opposing counsel could discern how long I had worked on the report. If it were a brief that I had prepared as an undisclosed coun-

Figure 1



Created: Friday, August 19, 2005 1:38:00 PM
Modified: Saturday, October 22, 2005 2:39:39 PM
Accessed: Saturday, October 22, 2005 2:39:39 PM
Printed:

Last saved by: Mercer Law School
Revision number: 44
Total editing time: 205 Minutes

Statistics:

Statistic name	Value
Pages:	15
Paragraphs:	192
Lines:	406
Words:	3417
Characters:	18294
Characters (with spaces):	21626

[21] I have only shown the screen for one of the five tabs:

> Each selection shows different information. Word generates much of this metadata automatically. The General selection shows the date and time the document was created (and modified and accessed), the size of the document, and the location of the document. The Summary selection shows the title of the document, the author's name, and the author's company, among other things. Users can also manually add comments about the document into fields under the Summary tab. Under the Statistics tab, anyone with access to the document can find the amount of time spent editing it, the name of the person who last saved it, the number of revisions, the date it was printed, and word count information. The Custom selection shows other documentation, such as the typist's name, the names of people the document was forwarded to, and the name of the client.

Levitt & Rosch, *supra* note 9, at 39.

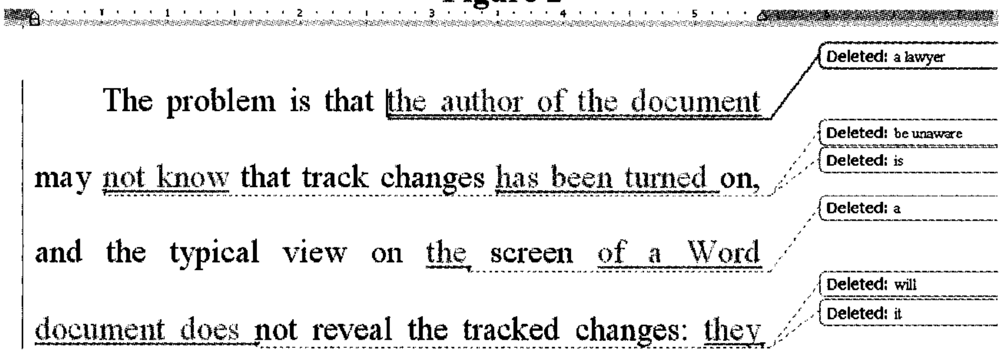
[22] To be clear, the file could simply have been open on the screen for 205 minutes; the amount of time indicated does not necessarily mean that I was working on the file for all of those 205 minutes. It could simply have been open while I was teaching class, for example. Conversely, I could have been working on a hard copy for several more hours.

sel, and then counsel of record had forwarded the document, my identity would be revealed.[23] Metadata matters.[24]

More troubling than metadata is the other data that can accompany a Word file. Foremost, "Track Changes" is a feature that creates a record of every change made to a file. Its many uses include lawyers who exchange drafts of contracts, as mentioned in the introduction, can turn on track changes so that it is easy to spot revisions made to a proposed contract during negotiations; word processing personnel may turn on track changes so that they can review and ensure that they have made each handwritten edit desired by a lawyer; a co-author can turn on track changes to monitor edits; and so on.[25]

The problem is that the author of the document may not know that "Track Changes" has been turned on, and the typical view on the screen of a Word document does not reveal the tracked changes. The changes will be "invisible." For example, I wrote this paragraph, and then went back and turned on track changes.[26] What you are reading now is the way the paragraph looked when I was finished editing it. Figure 2 shows what it looked like on October 23, 2005, with "Track Changes" turned on.

Figure 2



The problem is that the author of the document may not know that track changes has been turned on, and the typical view on the screen of a Word document does not reveal the tracked changes: they

Deleted: a lawyer

Deleted: be unaware

Deleted: is

Deleted: a

Deleted: will

Deleted: it

If I were to transmit the file that contains this Article to someone, he could easily reveal the changes and see the revisions to this document. If this were a contract, that could reveal to an opposing party revisions I had made to key terms of the proposed contract.[27]

[23] The kind and amount of information stored in the "Properties" file can be customized. To see whether your version has been customized, click on the "Custom" tab at the top of the "Properties" dialog box.

[24] There are a number of other sources of metadata. For example, other tabs in the "Properties" pop-up box will show where the file was stored on my hard drive and other information.

[25] *See generally* James Veach, *Commutation Agreements: Drafting a Clear and Comprehensive Contract*, 879 PLI/COMMERCIAL LAW PRACTICE COURSE HANDBOOK SERIES 467 (2003) (explaining that track changes can be used in the drafting process to create better documents).

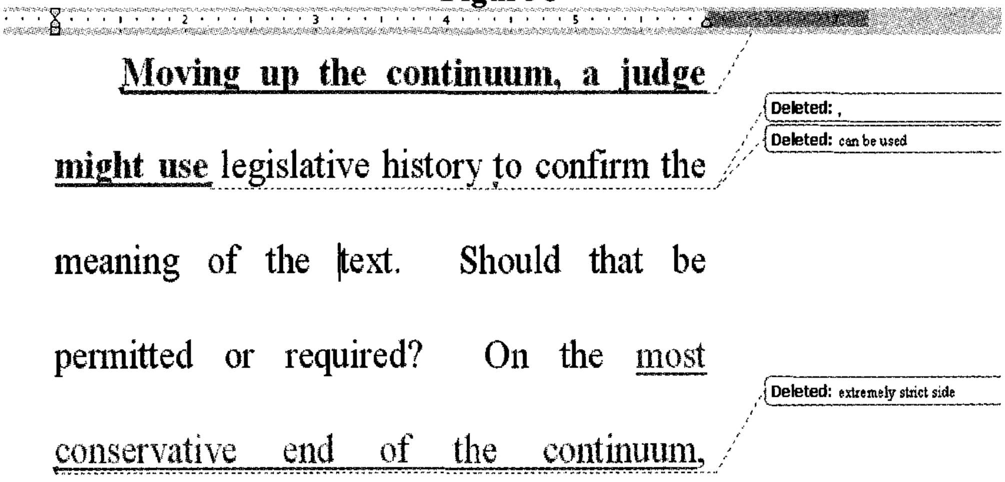
[26] In order to turn on track changes, go to the "Tools" menu and to "Track Changes." In order to see whether an open document contains tracked changes, turn on track changes, and then ensure that you are viewing the "Final Showing Markup."

[27] *See* Zall, *supra* note 17, at 55-56 (collecting hypotheticals on how metadata could harm clients and lawyers when exchanged with opposing counsel).

Another form of embedded Word data is created by the use of "Fast Saves." If "Fast Saves" is enabled,[28] then "deleted information remains hidden within the document."[29] Opposing counsel who receives a file that has been created with "fast saves" enabled can easily open the document and see all revisions.[30]

Another form of embedded data that can accompany Word documents is "Comments." Comments are incredibly useful for collaborative preparation of documents. For example, I am working with a colleague on a book on statutory interpretation. Each of us can make a comment to the other to explain the reason for a suggested a revision, inclusion of a certain concept, or the need for further clarification on some portion of the book. Those comments are embedded with the file and accompany it whenever we exchange the file. Figure 3 is a screen shot of a few lines from a chapter opened in Word with "View" set to "Showing Final Markup." Notice also that the "Track Changes" information is displayed:

Figure 3



Moving up the continuum, a judge might use legislative history to confirm the meaning of the text. Should that be permitted or required? On the most conservative end of the continuum,

Deleted: ,

Deleted: can be used

Deleted: extremely strict side

A final example is "Versions." If "Versions" is enabled, then embedded with the file are all prior versions of the document. Each time it is saved, a new version is created and saved. Thus, once again if the file is transmitted to opposing counsel, she can view every prior version of the document.[31]

[28] This is done by selecting "Save As" from the "File" menu, then selecting "Tools," and then "Save Options." One option is "Allow Fast Saves." Fast Saves is "very useful in the event of hardware failure because it reduces the chance of losing changes to a document." Toby Brown, *Special Handling: How Paper and Electronic Files Differ*, 21 GPSOLO Sept. 2004, at 23. *See also* Hoenig, *supra* note 10, at 52 (explaining that while "Fast Saves" "makes saving a document faster . . . the time saving results . . . from the fact that text that has been deleted while editing the document is not actually deleted from the electronic file that produces the document.").

[29] Brown, *supra* note 28, at 23.

[30] *Id.* at 22-23.

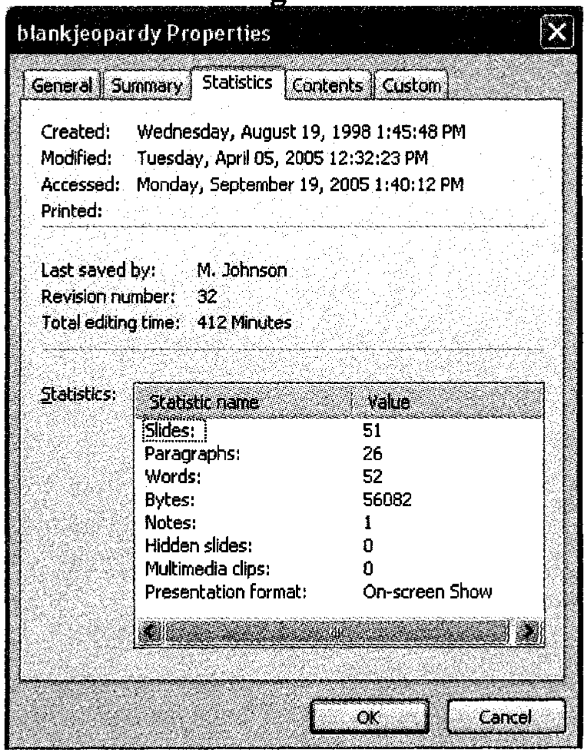
[31] *See* Zall, *supra* note 17, at 54-55. Various document management programs may impact this function. A lawyer in a firm using document management software should consult his IT department.

All of these features are useful to lawyers, their secretaries and their IT (information technology) staff. Lawyers need to be aware of the fact that these tools embed data with the file. Further, they also need to recognize that their staff may enable certain features without the lawyer's knowledge.[32] For example, a good secretary may enable "Track Changes" so that he can double-check that all hand-written changes have been made. If the lawyer is unaware of the enablement of these features, and if the secretary doesn't appreciate the problems created by transmitting the file with track changes still embedded, then disaster can strike.

2. *Other Microsoft Programs*

Like Word, other Microsoft products contain embedded data. For example, PowerPoint contains a "Properties" file. I downloaded from the Internet a blank "Jeopardy" file and the Properties from it reveals metadata shown in Figure 4.

Figure 4



Created: Wednesday, August 19, 1998 1:45:48 PM
Modified: Tuesday, April 05, 2005 12:32:23 PM
Accessed: Monday, September 19, 2005 1:40:12 PM
Printed:

Last saved by: M. Johnson
Revision number: 32
Total editing time: 412 Minutes

Statistics:

Statistic name	Value
Slides:	51
Paragraphs:	26
Words:	52
Bytes:	56082
Notes:	1
Hidden slides:	0
Multimedia clips:	0
Presentation format:	On-screen Show

In addition, "Speaker's Notes" are a part of PowerPoint files. Speaker's Notes are text that is not visible when a presentation is projected but which are visible to the speaker or can be printed out. They accompany the file when transferred unless removed beforehand.

[32] Model Rule 5.3(b) requires lawyers with direct supervisory authority over a nonlawyer to "make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer." The lawyer can, under some circumstances, be responsible for the nonlawyer's conduct. *See* MODEL RULES OF PROF'L CONDUCT R. 5.3 (2004).

3. *Corel Word Perfect*

Not only Microsoft products contain embedded data. Corel WordPerfect contains a "Properties" file that is somewhat less descriptive than Microsoft's.[33] Less information is, in the default mode, embedded in the "Properties" file than in Word. However, as in Word, this feature can be customized to include a variety of information, such as who received blind copies of the document.[34] Disclosing to the other side who received blind copies of a document obviously defeats the purpose of sending blind copies.

In addition, WordPerfect contains a "Multiple Undoes" feature. When "Multiple Undoes" is enabled, the file is accompanied by embedded data that allows the recipient to "Undo" a large number of revisions to the document. The recipient might, for example, be able to "Undo" changes to a proposed settlement agreement to see how much the plaintiff's opening offer was, and compare that to the amount actually mentioned in the first draft.

4. *Adobe Acrobat*

As noted above, many contend that one way to avoid transmitting embedded data is by converting the file into portable document format (".pdf").[35] This is only partly true: a Word document saved into .pdf format will no longer carry with it the data embedded by the Word program.[36] However, there are several caveats.

First, if the document is converted into .pdf format in the "View Final With Markup" setting, then the resulting .pdf document will show the comments and changes. Second, the document will still contain metadata: however, it will be the metadata created by Adobe Acrobat, not Word.[37]

Even Adobe .pdf documents have embedded data, though less so than Word or WordPerfect. For example, I converted a later version of this Article into a .pdf file, and Figure 5 represents the metadata that accompanied it:[38] There is clearly less metadata, but nonetheless the author, the time of creation, and the time of modification are visible.

Others have suggested that converting the file to "rich text format" (".rtf") eliminates embedded data.[39] This is true only in part: the information in "Properties" will be deleted and will reflect only the information pertaining to the file after it was converted to .rtf; however, if the original

[33] In WordPerfect, "Properties" is located on the File menu.

[34] While in the "Properties" dialog box, select "Set Up" to view the possible customized features. Word processing personnel may turn on some of these options without the lawyer knowing.

[35] Generally, this means "Printing" the document to Adobe distiller.

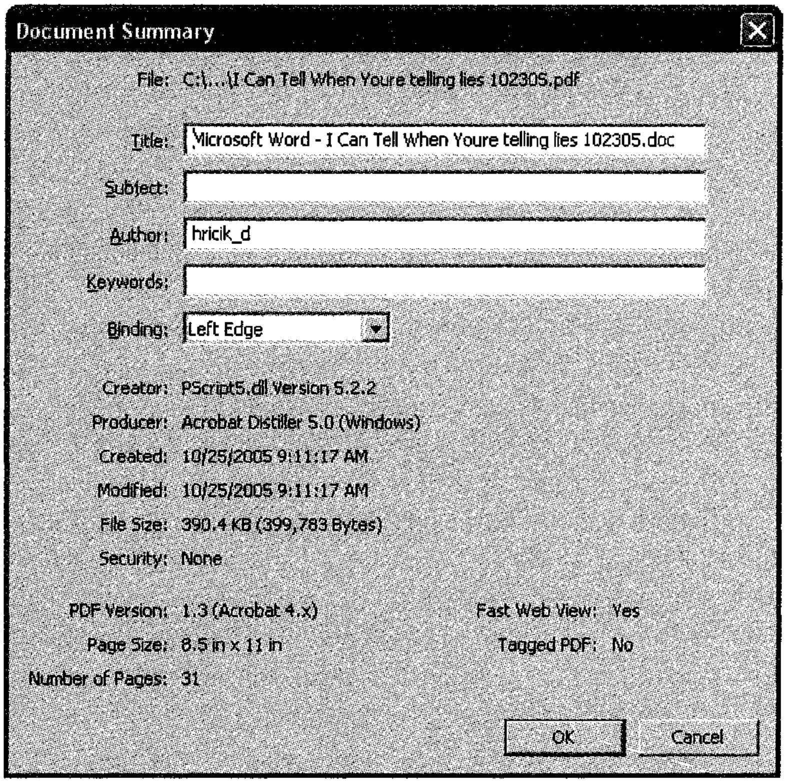
[36] *See* Adobe Portable Document Format, www.adobe.com/products/acrobat/adobepdf.html (last vistied Mar. 6, 2006).

[37] To view this embedded data, go to the "File" menu, then to "Document Properties."

[38] Metadata can be viewed under "File" and then "Document Properties."

[39] *See, e.g.*, Krause, *supra* note 6, at 26 ("Microsoft Word users can easily strip out much of a document's metadata by saving it in the Rich Text Format, or .rtf."); Levitt & Rosch, *supra* note 9, at 40.

Figure 5



File: C:\...\I Can Tell When Youre telling lies 102305.pdf

Title: Microsoft Word - I Can Tell When Youre telling lies 102305.doc

Subject:

Author: hricik_d

Keywords:

Binding: Left Edge

Creator: PScript5.dll Version 5.2.2

Producer: Acrobat Distiller 5.0 (Windows)

Created: 10/25/2005 9:11:17 AM

Modified: 10/25/2005 9:11:17 AM

File Size: 390.4 KB (399,783 Bytes)

Security: None

PDF Version: 1.3 (Acrobat 4.x)

Page Size: 8.5 in x 11 in

Number of Pages: 31

Fast Web View: Yes

Tagged PDF: No

document had been created with "Track Changes" on, the resulting rich text document will continue to reveal tracked changes. Converting to .rtf is not a thorough solution.

Given the ubiquity of embedded data, what must lawyers who send it, or receive it, do?

III. The Ethics of Embedded Confidential Information

This section analyzes the ethical principles implicated by the creation and transmission of embedded confidential information.

A. The Duty to Avoid Disclosing Embedded Confidential Information

A lawyer representing a client must use reasonable care to avoid inadvertent disclosure of confidential information.[40] Thus, two issues are presented: whether embedded data is "confidential information" and whether it violates a duty of care to transmit embedded data.

With respect to the issue of whether embedded data is "confidential information," it is important at the outset to emphasize the distinction between the duty of confidentiality and the attorney-client privilege. The attorney-

[40] *See* Model Rules of Prof'l Conduct R. 1.6 (2004).

client privilege is solely a rule of admissibility at trial,[41] while the duty of confidentiality has nothing to do with trial admissibility.[42] The duty of confidentiality can be implicated when that of privilege is not because "confidences" include, but are not limited to, "privileged" information.[43] Therefore, the appropriate question with respect to the transmitting lawyer's duty of care is not whether embedded data is privileged, but whether it is "confidential."

The scope of the duty of confidentiality is broad,[44] covering any information "relating to the representation of a client."[45] The definition of confidential information clearly includes, but is not limited to, privileged information.[46] Beyond that, it also requires protection of information which itself is not confidential but which could lead to disclosure of confidential information: "This prohibition also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person."[47]

For these reasons, it is clear that lawyers have an obligation to protect all information relating to the representation of a client.[48] Obviously, they cannot intentionally disclose confidential information. Thus, a lawyer who knows of the presence of embedded data that consists of "confidential information" must remove it. For example, where data consist of track changes that reveal prior substantive revisions suggested by a client, the lawyer should avoid transmitting the document without first removing the embedded data, which likely constitute privileged information. Similarly, where the "Properties" in a document could reveal protected information—such as the fact that the document was authored by undisclosed co-counsel—the embedded data should be removed.[49] A lawyer who transmits a document knowing that it contains embedded client confidences violates the duty of confidentiality.

[41] *See* Purcell v. Dist. Attorney for Suffolk County, 676 N.E.2d 436 (Mass. 1997) (holding that information which was subject to disclosure as "not confidential" was still privileged).

[42] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 (2004).

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] "The confidentiality rule... applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source." MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 3 (2004).

[47] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 4 (2004).

[48] *Id.*

[49] It is extremely doubtful that *all* embedded data is a "client confidence." For example, the properties file shown from the .pdf version of this Article merely discloses the time and the fact that I wrote the document. It stretches the boundaries of "confidential" to deem those items confidential in most imaginable circumstances. *See also* Hoenig, *supra* note 10, at 51 (noting that the .pdf file will "identify the user who prepared the document and the path to where the document is stored. This metadata, however, should very rarely be a problem."). Suppose, however, that the path reveals the name of an undisclosed principal who is interested in acquiring property without its identity being disclosed; even this minimal amount of embedded data could in some circumstances constitute confidential information.

The duty of confidentiality is not limited to intentional disclosure.[50] In addition to having an obligation not to knowingly reveal confidential information, lawyers also have a duty to avoid inadvertent disclosure of confidential information.[51] The fact that reasonable steps are required raises the question of whether a lawyer violates the duty of care by not discovering the complete nature of the file transmitted.

Do lawyers violate the duty of confidentiality if they knowingly transmit a document but are ignorant of the embedded confidential information? There are several ways this could occur, each of which requires different analysis.

First, the lawyer could have been aware of the presence of embedded data, and taken reasonable efforts to remove it, but nonetheless failed because of technological or user-related failures. It may be, for example, that a lawyer thought she removed the comments from a document, but had failed to "View" it in a way that would reveal the still-present comments. Similarly, the lawyer may have been aware that the program created embedded data but believed that the functionalities that create such data had been disabled.

It is easy to make mistakes even when exercising reasonable care and it seems that even experts disagree on whether particular approaches avoid disclosure of all embedded data.[52] For these reasons, it is doubtful that a lawyer who either takes reasonable steps to remove metadata or who avoids creating it in the first place violates the standard of care or the duty of confidentiality. Obviously, this is a fact-intensive inquiry, but lawyers are not required to meet an unattainable standard.

Second, the lawyer could have created a file not knowing that it contained embedded data because the lawyer was unaware that the software created such data. Whether those circumstances violate the duty of confidentiality turns on the question of whether, at the time the document was created, a lawyer "should have known" of embedded data.

Clearly, lawyers have an obligation to take reasonable care to protect client confidences, a duty which includes an obligation to "stay abreast of technological advances and the potential risks."[53] While some authors have essentially argued that "everyone knows" about embedded data, and so lawyers "should know" about it, in my own experience the opposite is true. In speaking about this issue to nearly 1,000 lawyers, it was apparent that the

[50] MODEL RULES OF PROF'L CONDUCT R. 1.6 (2004).

[51] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 16 (2004) ("A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.").

[52] As noted above, for example, some say that converting a document to .pdf format removes all metadata, when in fact as shown here it simply replaces it with a different, lessened amount of metadata. *See supra* notes 35 to 39 and accompanying text.

[53] N.Y. St. Bar Ass'n Comm. on Prof'l Ethics Op. No. 782 (Dec. 8, 2004). *See* Zall, *supra* note 17, at 56 (reasoning that attorneys must "exercise reasonable care by familiarizing themselves with the attendant risks associated with metadata and taking affirmative steps to eliminate the risks").

vast majority had never heard of embedded data, let alone how to avoid creating it or how to remove it.[54] Confirming my less-than-scientific poll, documents routinely show up on the web which contain embedded data, many of which were posted by lawyers who ostensibly should have been aware of embedded data.[55]

These facts suggest that lawyers are not aware of metadata; whether their failure is due to lack of reasonable care is not yet clearly settled.[56] The only authority on this point rejected imputing lawyers with knowledge of embedded data.[57] Obviously, as awareness of embedded data spreads, it will become more difficult for lawyers to contend that transmitting embedded data did not violate the duty of care. As a result, at some point—perhaps soon—lawyers will not be able to avoid negligence claims by pleading ignorance of the risks that this information creates.[58] However, until that time, whether a lawyer "should have known" will remain a fact-intensive issue, turning on the nature of the practice, the type of representation, and the importance of the information at issue.

The problem, of course, is that a lawyer does not want to be the "test case" which announces that this time has come. Where a lawyer knows or should know of the presence of embedded confidential information, the lawyer must take steps to avoid its disclosure.[59] The next section addresses how to avoid intentionally sending embedded confidential information.

1. *How to Remove or Avoid Creating Embedded Data*

There are several ways to address inadvertent transmissions of embedded data. This section surveys technical and other means to eliminate or at least reduce the likelihood of an inadvertent transmission occurring.[60]

[54] *See also* Hoenig, *supra* note 10, at 51 ("Many, if not most, lawyers are unaware that documents prepared with word processing software often contain information invisible to the normal document reader, particularly if the document is read only from a paper printout.").

[55] *See* Krause, *supra* note 6, at 27 (describing example containing track changes and comments in Word document).

[56] As noted below, this lack of certainty about whether lawyers know or should be deemed to know about embedded data complicates the question of whether lawyers who receive files with their opponents' embedded confidential information have an obligation to destroy the file, or avoid reading it. *See infra* notes 71-98 and accompanying text.

[57] N.Y. St. Bar Ass'n Comm. on Prof'l Ethics Op. No. 782 (Dec. 8, 2004). *See* Zall, *supra* note 17, at 56 (reasoning that attorneys must "exercise reasonable care by familiarizing themselves with the attendant risks associated with metadata and taking affirmative steps to eliminate the risks.").

[58] Some say that day came nearly two years ago. Vincent Polley, chair of the ABA's Cyberspace Law Committee, has been quoted as saying that lawyers can no longer "plead ignorance when it comes to this stuff anymore." Krause, *supra* note 6, at 27.

[59] *See* Walker, *supra* note 9, at 331 ("[W]hen a lawyer transmits a document knowing that its metadata reflects client confidences . . . and that the non-lawyer recipient is able to reveal the hidden text, and does not take protective measures to strip the document of metadata, the lawyer's transmission . . . may constitute a knowing disclosure of client confidences . . . .").

[60] *See generally* Levitt & Rosch, *supra* note 9, at 40 (describing various means to remove metadata, including some of those discussed here); Storm Evans, *How to Commit Malpractice With a Computer*, 29 L. PRAC. MGMT. 56, 56 (2003) ("If you must e-mail or otherwise deliver a Word document, consider using macros or a utility program to strip away the metadata").

a. Avoid Creating Embedded Data

One way to avoid disclosure of embedded confidential information is to not create it in the first place. Microsoft has in recent years created updates that allow users to avoid creating embedded data. While this is obviously a sure fix, it also means that lawyers cannot take advantage of the power that functionalities such as "Track Changes" bring to the program. A lawyer could not, for example, exchange revisions of a document with her client using "Track Changes" and "Comments" to render the revision process more efficient and certain.

Nonetheless, if there is no embedded data, it cannot be transmitted. Thus, creating documents with "Fast Saves" off, "Versions" disabled, and without any data in the "Properties" file meets this goal.[61] Similarly, PowerPoint can be configured to remove personal data from the "Properties" file.[62] Finally, in WordPerfect, one can ensure that "Multiple Undoes" is turned off [63] and set the program so that the properties are deleted from the document.[64]

b. Removing Embedded Data

Because embedded data can contain confidential client information, lawyers who transmit files should consider removing it.[65] There are various steps that can reduce, or eliminate, metadata. Because reasonable care is necessary, the nature of the communication will indicate what steps are required for particular communications or practices.

Saving a document into .pdf format reduces the amount of metadata but does not eliminate it entirely. [66] For many purposes, simply saving a document into .pdf format may suffice. However, documents in .pdf format can-

[61] The easiest way to avoid creating data with the "Properties" file in Microsoft Word is:

1. On the Tools menu, click Options.
2. On the Security tab, select the "Remove Personal Information From File Properties On Save" check box under "Privacy Options," and then click OK.

With this option turned on, the program will automatically remove all metadata from the properties file each time the file is saved. *See* Microsoft.com, How to Minimize Metadata in Word 2003, http://support.microsoft.com/default.aspx?scid=kb;en-us;825576 (last visited Feb. 20, 2006).

[62] In PowerPoint, under the "Tools" menu select "Options" and then select the "Security" tab and ensure that the box to remove personal data is selected.

[63] Under the "Edit" menu, go to "Undo/Redo History," then click "Options" and ensure the box for "Save Undo/Redo History With Document" is not selected.

[64] To do this, when the document is complete, go to File/Properties, then click the "Options" button and select "Delete Summary From Document" and then confirm that choice. Notice that you must do this at the last save.

[65] *See* Beckerman-Rodau, *supra* note 19, at 32-33 (suggesting that lawyers should consider removing metadata); Hoenig, *supra* note 10, at 51.

[66] *See* Jason Krause, *Guarding the Cyberfort,* 39 ARK. LAW. 24, 31 (2004). Suggestions, however, that .pdf files contain *no* metadata are incorrect. *E.g.,* Hoenig, *supra* note 10, at 52-53; RONALD E. MALLEN & JEFFREY M. SMITH, LEGAL MALPRACTICE § 2.26 (2005) (stating that conversion from Word to .pdf "could eliminate meta-data information"). As noted above, Adobe .pdf files contain metadata; thus, saving a Word file as a .pdf file will simply result in *different* metadata being transmitted.

not be easily modified, which may reduce the efficiency and functionality of document exchanges.

Each of the programs has add-ons and other utilities to remove metadata.[67] As you can see, they require several steps per document, and pur-

[67] There are different approaches for different programs. Here are some basics:

Microsoft Office XP

Microsoft created a Remove Hidden Data tool add-in for Word 2003, Excel 2003, PowerPoint 2003, Word 2002, SP2 or later, Excel 2002, SP2 or later, and PowerPoint 2002, SP2 or later. Microsoft.com, The Remove Hidden Data Tool for Office 2003 and Office XP, Microsoft.com, The Remove Hidden Data Tool for Office 2003 and Office XP, http://support.microsoft.com/kb/834427#top (last visited Feb. 20, 2006). This add-in removes comments, previous authors and editors, user names, personal summary information, revision marks, deleted text, versions, VB Macros, document ID numbers, routing slips, e-mail headers, scenario comments, and unique identifiers in Office 97 documents. *Id.* The add-in and additional information may be found on this same website. Microsoft.com, Office 2003/XP Add-in: Remove Hidden Data, http://www.microsoft.com/downloads/details.aspx?FamilyId=144E54ED-D43E-42CA-BC7B-5446D34E5360 (last visited Feb. 20, 2006).

You can also show and remove hidden text:

1. On the Tools menu, click Options, and then click the View tab.
2. Click to select the Hidden text check box, and then click OK.
3. On the Edit menu, click Replace.
4. Click More to expand the dialog box.
5. Click anywhere in the box next to Find what.
6. Click the Format button, and then click Font.
7. Click to select the Hidden check box, and then click OK.
8. Click Replace All.

Microsoft.com, How to Minimize Metadata in Word 2003, http://support.microsoft.com/default.aspx?scid=kb;en-us;825576 (then follow the "How to Search for and Remove Text That Is Formatted As Hidden" hyperlink) (last visited Feb. 20, 2006).

Once you are finished removing hidden text, you can hide hidden text:

1. On the Tools menu, click Options, and then click the View tab
2. Click to clear the Hidden text check box, and then click OK.

Id. (Instructions on how to manually remove your user name, personal summary information, comments, headers and footers, revision marks, hyperlinks, styles, old file versions, links from field codes, template names and locations, routing slip information, VB code names and references, network and hard disk information, and document variable information may also be found at this site).

PowerPoint 2003

1. On the File menu, click Save As.
2. In the Save As dialog box, click Tools, and then click Security Options.
3. On the Security tab, click to select the Remove personal information from file properties on save check box, and then click OK.

Microsoft.com, How to Minimize Metadata in PowerPoint 2003 Presentations, http://support.microsoft.com/default.aspx?scid=kb;en-us;826825 (last visited Feb. 20, 2006) (additional instructions on manually removing metadata from PowerPoint 2003 documents may also be found at this cite).

WordPerfect 12

To find and remove all hidden text

1. Click View ▶ Reveal Codes.
2. Click Edit ▶ Find and Replace.
3. In the Find and Replace dialog box, click Match ▶ Codes.
4. In the Codes dialog box, choose Hidden On from the Find codes list.
5. Click Insert & Close.
6. In the Find and Replace dialog box, choose Nothing from the Replace with list box.
7. Click Replace All.
8. Click Close.

Corel.com, Minimizing Metadata in WordPerfect 12 Documents, http://www.corel.com/content/pdf/wpo12/Minimizing_Metadata_In_WordPerfect12.pdf. at 6 (last visited Feb. 20, 2006).

To accept or remove document revision annotations

1. Click File ▶ Open.
2. Locate the file that has been reviewed, and click Open.
   The Review Document dialog box will open.

portedly not all embedded data is necessarily scrubbed from the document by taking all of these steps.[68] As a result, reliance on commercial software to do the job may be required under some circumstances, especially where the information is particularly valuable or sensitive.[69]

c. *Agreement with Counsel*

A final, less technical manner of avoiding the problems associated with embedded data is to have an agreement in place with opposing counsel that any transmission of embedded data is not intentional and will require the opposing party to return files containing embedded data.[70] Obviously, this

3. Click Author.
4. On the Document Review toolbar, click one of the following buttons:
   - [symbol omitted] Inserts the currently selected annotation into the text of the document
   - [symbol omitted] Inserts all annotations into the document text
   - [symbol omitted] Deletes the currently selected annotation
   - [symbol omitted] Deletes all annotations from the document text
5. Click Close.

Id. at 7.

To disable the Undo/Redo history

1. Click Edit ▶ Undo/Redo History.
2. Click Options.
3. Disable the Save Undo/Redo items with document check box.
4. Click OK.
5. Click Close.

Id. at 9.

To remove summary information from an older document or template

1. Click File ▶ Open.
2. Choose the file you want to open, and click Open.
3. Click File ▶ Properties.
4. Click the Summary tab.
5. Delete any information that should not be distributed with the document ...
6. Click OK.
7. Click File - Save.

Id. at 10-11. There are also instructions on how to remove comments, styles, names and initials, hyperlinks, header and footer information, linked objects and instructions on publishing the document as a .pdf. *Id.* at 3.

[68] *Id.* at 4.

[69] There are a number of commercial "metadata scrubber" programs available: *see* Hoenig, *supra* note 10, at 51 (explaining that a Google search of "clean metadata from word documents" garnered 18,000 hits); Levitt & Rosch, *supra* note 9, at 41 (discussing various programs). The programs below relate to Microsoft products. I was unable to find removal tools for WordPerfect. I have never used any of these but list them for your convenience.

Metadata Analyzer, *at* http://www.smartpctools.com/metadata/.
Document Trace Remover 2.0, *at* http://www.smartpctools.com/trace_remover/.
TRACE!, *at* http://www.workshare.com/products/trace/.
Workshare Hygiene, *at* http://www.workshare.com/security-technology.aspx.
Metadata Assistant, *at* http://www.payneconsulting.com/products/metadataretail/.
Out-of-Sight, *at* http://www.softwise.net.
ezClean, *at* http://www.kklsoftware.com/products/ezClean/details.asp
BEC LegalBar Metadata Scrubber, *at* http://www.beco.com/lsy/lsylegspeclegbarmetadata.asp
iScrub, *at* http://www.esqinc.com/?p=products&id=2

[70] *See generally* Thomas E. Spahn, *Litigation Ethics in the Modern Age*, 33 BRIEF 12, 16-17 (Winter 2004) (suggesting such agreements in order to address the risks of inadvertent transmission of

turns on the trust of counsel, and where the mere viewing of the information "lets the cat out of the bag," such agreements may not suffice. Either ensuring that embedded data is not created or that it is stripped out before a file is sent will, in most circumstances, be the only effective way to address the problems of embedded data.

d. Using Paper

Based upon experience and discussion with others, there is not one surefire way to remove all embedded data all of the time. Transmitting paper, not electrons, may be the only certain way to avoid unknowingly transmitting embedded confidential information. Obviously, though, that defeats the functionalities of software and denies lawyers the convenience of the Internet.

B. The Obligations of Lawyers Who Receive Inadvertently Transmitted Information from Opposing Parties

The foregoing shows that it is unclear whether lawyers who transmit embedded data do so "intentionally," or in violation of the duty of confidentiality. Further, some embedded data may constitute privileged or confidential information.[71] It is therefore possible that a lawyer can receive embedded data from opposing counsel that is privileged or confidential and be unable to tell whether it occurred intentionally (which seems doubtful) or inadvertently (which is more likely). In that case, it will be unclear whether the transmitting lawyer sent the embedded data as the result of failing to scrub the data, inadvertently using the scrubber, inadvertently allowing the data to be created in the first place, or ignoring the existence of embedded data. What must the recipient do?

1. The General Duties of Lawyers Who Receive Misdirected Privileged or Confidential Information.

There is an entire body of law directed to the question of the duties of a lawyer who receives a communication by mistake. In some jurisdictions, the lawyer is free to use the materials, even if they contain privileged or confidential information, while in other jurisdictions the recipient has an ethical duty to notify the transmitting lawyer of the mistake and, in some jurisdictions, follow the transmitter's instructions on how to proceed next.[72]

paper documents); Zall, *supra* note 17, at 58 (noting that a benefit of proposing such an agreement is that it will alert the lawyer as to opposing counsel's attitude toward review of embedded data).

[71] Zall, *supra* note 17, at 55.

[72] *See* N.Y. City Bar Ass'n Comm. on Prof'l & Judicial Ethics Op. 2003-04 (Dec. 2003) (discussing differing approaches and disagreements on this issue). *See generally* Douglas R. Richmond, *Key Issues in the Inadvertent Release and Receipt of Confidential Information,* 72 DEF. COUNS. J. 110 (2005); Walker, *supra* note 9, at 334-36; Zall *supra* note 17, at 57.

It is important to note that an ethical responsibility arises when a lawyer receives information that he should know was not intended for him: "A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender."[73] A comment to the rule explains that a lawyer who knows or reasonably should know that a document was sent inadvertently should "promptly notify the sender in order to permit that person to take protective measures."[74]

Significantly, at least under Model Rule 4.4(b), the duty is not limited to documents which contain privileged or confidential information, but instead applies whenever a lawyer receives a document that he should know was sent inadvertently, regardless of the content.[75] Nothing in Model Rule 4.4(b) limits its application to documents that contain privileged or confidential information.[76] Thus, in jurisdictions in which Model Rule 4.4(b) is adopted, a lawyer who receives "a document" inadvertently must notify the sender.[77] Whether intentional receipt of a document that inadvertently contains embedded data implicates this rule is discussed below.

Other authorities take a narrower, or at least different, approach to this issue than Model Rule 4.4(b).[78] Ethics opinions in other jurisdictions impose duties upon lawyers who receive inadvertently transmitted documents from another lawyer, but often only if the document contains "privileged" or "confidential" information.[79] These bar opinions are largely imprecise, based on indeterminate rules (whether, for example, the lawyer "should know" the information was sent inadvertently), not uniform among jurisdictions, and not in effect in every state.[80] In these jurisdictions, a lawyer who receives a document containing embedded data has a duty to notify the party who transmitted the document only if the transmission is "inadvertent" *and* embedded data is "privileged" or "confidential."

[73] MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2004).

[74] MODEL RULES OF PROF'L CONDUCT R. 4.4(b) cmt. 2 (2004).

[75] In this regard, the rule is broader than some ethics authorities, which impose an obligation to take action only if the information is confidential or privileged. *See, e.g.*, Ethics Op. 2003-04, *supra* note 72 (concluding that when a lawyer receives misdirected documents containing "confidences" or "secrets," certain obligations arise). Thus, in jurisdictions which impose a duty only when certain types of information are disclosed, a threshold issue of whether the embedded data reflects privileged or confidential information arises. In the abstract, metadata is not likely to reflect privileged information, but comments and track changes likely do. Whether a particular document's embedded data is "privileged" or "confidential" obviously turns on the specific facts.

[76] *See* MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2004).

[77] *Id.*

[78] *E.g.*, Pa. Ethics Op. 2005-22 (Apr. 2005) (discussing Pennsylvania's adoption of Rule 4.4(b)).

[79] Ethics Op. 2003-04, *supra* note 72 (concluding that a lawyer who receives misdirected documents must, if they contain "confidences" or "secrets," advise the sender of the mistake, unless the lawyer has a good faith belief that a tribunal before which a dispute is pending will conclude confidentiality has been waived); N.Y. County L. Ass'n Ethics Comm. Op. 730 (holding that lawyers should assist in preserving confidences of sender of inadvertently privileged documents); ABA Ethics Op. 92-368, *supra* note 1 (holding that recipient of misdirected communication should advise sender of the mistake and abide by its instructions).

[80] *See* Ethics Op. 2003-04, *supra* note 72 (discussing variations and disagreements on the duty).

Thus, under either approach, the threshold question is whether the intentional transmission of a document that inadvertently contains embedded data is "inadvertent for purpose of these rules." Under Model Rule 4.4(b), that alone is sufficient to trigger the notification obligation.[81] Thus, the next section addresses what inadvertence means in the context of embedded data.

2. *Is Transmission of Embedded Data Inadvertent?*

It is important to be clear about what was done inadvertently and what was done intentionally. The assumption is that the lawyer who created the file *intended* to send it to the lawyer who received the file but unintentionally included embedded data. Can this be characterized as "inadvertent" transmission when it is clear the lawyer *intended to transmit the file*?

The authorities generally recognize two forms of inadvertent transmission. One occurs when a lawyer inadvertently includes as a recipient an unintended person,[82] such as by sending a fax intended for a client to opposing counsel.[83] Lawyers must take reasonable precautions to prevent inadvertent transmission of confidential information to third parties, and especially, opposing counsel.[84] The harm, of course, is that inadvertent disclosure of privileged information can waive the privilege – or if not, it can let the cat out of the bag.[85]

Another form of transmission occurs when a person who lacks authority to do so intentionally transmits privileged information to an opposing party.[86] This has happened frequently when disgruntled employees mail opposing counsel privileged or work product documents.[87] It is more appropriately labeled unauthorized transmission, rather than unintentional transmission, since certainly the disgruntled employee intended to send the information, but was not authorized to do so.

[81] MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2004).

[82] The ABA mentioned inadvertent transmission of e-mail when analyzing waiver of privilege over a misdirected fax: "the availability of xerography and proliferation of facsimile machines and electronic mail make it technologically ever more likely that through inadvertence, privileged or confidential materials will be produced to opposing counsel by no more than the pushing of the wrong speed dial number on a facsimile machine." ABA Formal Op. 92-368, *supra* note 1 and accompanying text. *Accord* Fla. St. Bar Ass'n Comm. on Prof'l Ethics Op. 93-3 (Feb. 1, 1994) ("Such an inadvertent disclosure might occur as part of a document production, a misdirected facsimile or electronic mail transmission, a 'switched envelope' mailing, or misunderstood distribution list instructions.").

[83] ABA Formal Op. 92-368, *supra* note 1; *accord* Fla. Ethics Op. 93-3, *supra* note 82 ("Such an inadvertent disclosure might occur as part of a document production, a misdirected facsimile or electronic mail transmission, a 'switched envelope' mailing, or misunderstood distribution list instructions").

[84] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (2004) ("When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients.").

[85] *See In re* Sealed Case, 877 F.2d 976 (D.C. Cir. 1989) (inadvertently disclosing privileged information waives the privilege); Georgetown Manor v. Ethan Allen Corp., 753 F. Supp. 936 (S.D. Fla. 1991) (inadvertent disclosure can never waive privilege); Alldread v. City of Grenada, 988 F.2d 1425 (5th Cir. 1993) (inadvertent disclosure can sometimes waive privilege).

[86] *See, e.g., In re* Shell Oil Refinery, 144 F.R.D. 73 (E.D. La. 1992) (current employee of a party provided an adverse party with confidential documents belonging to his employer).

[87] *See, e.g., id.*

Although embedded data could be transmitted without authority, it is more likely to fall under the first type of inadvertent transmission. The analogy between transmission of embedded data and inadvertent transmission in the "real world" is fairly obvious: a lawyer intentionally sends a proposed contract to opposing counsel, but inadvertently includes a mark-up of the contract with handwritten comments received from the client. No one would contend that by intentionally transmitting the proposed contract, the lawyer intentionally transmitted the client's mark-up. The lawyer intended the transmission, but he did not intend to transmit the mark-up.

The distinction, of course, is that the embedded data is not a separate file, but is "in" the intentionally sent file. That is too fine a point, and conflates intentionally transmitting a "file" with intentionally transmitting the information the file contains. The transmission of embedded data should be found to be inadvertent.

As a consequence, in states that follow Model Rule 4.4(b), a lawyer who receives a file with embedded data is in a position where receipt alone triggers the rule. As a result, she cannot examine the data, and should notify the sender of its receipt.[88]

The only bar association to have addressed this issue agreed with this conclusion.[89] The New York State Bar Association reasoned that, although the transmitting lawyer intended to transmit the file, "absent an explicit direction to the contrary counsel plainly does not intend the lawyer to receive the 'hidden' material or information."[90] It then characterized the transmission as inadvertent, and the review as deliberate, in order to conclude that a lawyer cannot review embedded information; "it is a deliberate act by the receiving lawyer, not carelessness on the part of the sending lawyer that would lead to the disclosure of client confidences and secrets."[91] As a result, "attorneys who receive electronic documents from the opposing side and take affirmative steps of . . . mining the document for confidential metadata . . . run a substantial risk of" violating the ethics rules or becoming "the target of disqualification motions."[92]

Some lawyers who disagree with this conclusion apparently assume that the transmission was intentional, and thus not inadvertent. "The first thing [lawyers] often do when they get documents from the opposition is to look for metadata to see who last drafted it or look for embedded versions of earlier drafts."[93] To support this view, many contend that the transmission

[88] *See supra* notes 72-81 and accompanying text.

[89] N.Y. St. Bar Ass'n Op. 749 (Dec. 14, 2001).

[90] *Id.*

[91] *Id.*

[92] Zall, *supra* note 17, at 57-58. The party who sent the document could move to disqualify the lawyer in connection with the matter or substantially related matters, for example. *See* MODEL RULES OF PROF'L CONDUCT R. 1.9 (2004).

[93] Krause, *supra* note 66, at 31 (quoting Vincent Polley, Chair of the ABA's Cyberspace Law Committee) (bracketed material in original).

of embedded data is itself an intentional act, since "every one knows" embedded data exists.[94]

The problem is that whether the transmitting lawyer knew the information exists is irrelevant; instead, the question is whether the recipient should know that the transmission was inadvertent: "The issue thus becomes whether the Inquirer knows, reasonably believes or should know that the disclosure was inadvertent. If the disclosure was not inadvertent then the Rule [4.4(b)] does not apply."[95] Therefore, in jurisdictions which follow Model Rule 4.4(b), the fact that embedded data was inadvertently transmitted is, by itself, sufficient to trigger the obligations.

Under Model Rule 4.4(b), receipt of embedded data alone triggers the rule and is not limited to inadvertent receipt of documents with privileged or confidential information. Even in those states that limit the ethical obligations to the inadvertent receipt of communications that contain confidential or privileged information, some embedded data will likely be confidential or privileged. For example, every lawyer knows that the opposing side's client's comments on a proposed contract are information that should be kept confidential.[96] A lawyer, therefore, who knows that viewing the "tracked changes" in a document will reveal confidential information of the opposing party does not mean that the recipient can view that information. Indeed, it means the opposite:

> In this regard, information that is clearly identified as confidential in nature or appears on its face to be subject to the attorney-client privilege under circumstances that make it clear it was not intended for the receiving lawyer, should not be examined. The receiving lawyer should immediately notify the sending lawyer and abide by his instructions with respect to inadvertently disclosed privileged material.[97]

A lawyer who deliberately takes steps to view embedded data is engaging in a deliberate review of information that she ostensibly *knows* should have been removed, and which she *knows* is confidential, at a minimum. Further, the transmitting lawyer may not—and indeed, apparently did not—know of the existence of embedded data, or it would have been removed.[98]

[94] Some say that day has already come. For example, Vincent Polley, chair of the ABA's Cyberspace Law Committee has been quoted as saying that lawyers can no longer "plead ignorance when it comes to this stuff any more." Krause, *supra* note 6, at 27. *See* Levitt & Rosch, *supra* note 9, at 41 (explaining that if the New York opinion were written "today, it may not be as forgiving of a lawyer who fails to remove metadata before sending electronic documents to the opposition").

[95] Pa. Ethics Op. 2005-22, *supra* note 78.

[96] Hoenig, *supra* note 10, at 51 ("When drafting transactional documents, it is obviously undesirable to let the other side see what text was added or deleted . . . or what changes were being considered for addition or deletion to the last draft of a document sent to the other side that were not included. Disclosing such information to the other side can help it in its negotiation strategy").

[97] Sampson Fire Sales, Inc. v. Oaks, 201 F.R.D. 351, 362 (M.D. Pa. 2001).

[98] *See supra* notes 82 to 98 and accompanying text.

Therefore, a lawyer should not view embedded data in jurisdictions where any review of inadvertently transmitted documents is unethical or in jurisdictions that prohibit review of privileged or confidential information of the opposing party.

IV. An Important Conclusion

The conclusion that receipt of embedded data triggers ethical obligations in states that follow Rule 4.4(b), and that it triggers obligations in states that adopt the narrower approach to the problem when it contains privileged or confidential information, does not end the inquiry. The lawyer who receives the information can—and, perhaps must if the facts warrant—contend that the inadvertent transmission of the embedded data constituted a waiver of the protections.[99] There is nothing incompatible notifying the sender of receipt of a misdirected communication as required, and yet contending that privilege was waived due to that fact. Indeed, in order to satisfy both the ethical duties imposed in many jurisdictions and the duty of zealous representation of the recipient's client, the lawyer may need to avoid use of the document and request guidance from a court, if possible.

To return to our Macrosoft example, the lawyer who received the file with the embedded data may, depending on the jurisdiction's approach to the question of inadvertent receipt of documents, have an obligation to notify Macrosoft's lawyers of the transmission and, in some states, to follow their instructions on how to proceed. Nonetheless, the lawyer may be free to argue that privilege has been waived, and to litigate the issue.

Finally, a rather Kafka-esque point needs to be noted. Some lawyers, aware of embedded data, are planting false embedded data in order to mislead opposing counsel or to test whether opposing counsel is viewing this material inappropriately.[100] By planting false embedded data, these lawyers may be able to turn improper use of embedded data against those who do not follow their own ethical responsibilities.

Perhaps Macrosoft's lawyers had the last laugh. Or, perhaps they have themselves compounded the matter by making false statements to the opposing counsel.

[99] *See, e.g., Sampson Fire Sales, Inc.*, 201 F.R.D. at 360. (analyzing whether reasonable steps were taken to prevent inadvertent faxing of privileged letter to opposing counsel).

[100] *See* Krause, *supra* note 6, at 27.

Exhibit I

Metadata: The Ghosts Haunting e-Documents

By David Hricik and Chase Edward Scott

Metadata is "data about data."[1] Although it sounds quite modern, one form of metadata is no doubt familiar to every lawyer: the "fax band" on a document received by facsimile that shows the time and date that the fax was received, the number from which it came, and the number of pages sent. A fax band is metadata since it is data about data. Even this simple form of metadata may be important. It could show that a party's claim to not have received a document on a certain date is incorrect.

Metadata is not new, but it has become pervasive in the digital world in which lawyers (and their clients) live. Many programs commonly used in the office create data about data and then save that unseen information along with the visible text of the document in a single file. Put simply, "invisible fax bands" commonly accompany many of the electronic documents we create on a daily basis. This unseen information is typically transferred along with the document in which it is embedded unless removed prior to transmission. Generally, each time a file is transmitted, the invisible fax bands are also sent.

Rather than simply revealing seemingly innocuous information, such as the time and date that the file had been prepared, metadata often reveals much more. For example, many software programs permit an author to track changes to the text, to save multiple undoes in case the author later decides to undo revisions made long ago, or even to insert invisible comments into the file. Such data could reveal a wealth of information to recipients of the electronic file, potentially affecting significant negotiation positions, litigation strategies, and numerous other sensitive scenarios.

Recently, a lawyer relayed a story to one of the co-authors that demonstrates the risks of exchanging files with embedded data. In negotiating a contract against a well-known software maker that, for purposes of this article, will be called Mercer, the lawyers for each side used a common word-processing program, Microsoft Word, to edit and propose revisions to the contract. The lawyers used the program's track changes feature to allow the lawyers to see the specific changes proposed. They emailed the electronic drafts, complete with embedded data, back and forth to each other between rounds of revisions. After receiving one such draft from Mercer's counsel, the lawyer made a few easy mouse clicks to reveal, without using anything but Microsoft Word's inherent functions, "hidden" internal comments from Mercer's business personnel concerning terms of the contract, negotiating positions, and bottom lines. Had Mercer subsequently insisted that a non-compete clause would be needed to close the deal, the opposing lawyer would have been able to tell if the demand was simply a negotiating ruse. Clearly, metadata is an important consideration in today's legal environment.

This article explains how metadata is created and embedded in some popular programs and analyzes the ethical obligations to remove this embedded material from documents that lawyers create on their clients' behalf. Did Mercer's lawyers, for example, violate duties to their client by sending embedded data along with the text of the contract to opposing counsel? This article also provides a number of useful tips on how lawyers can remove metadata from documents created in some of the more popular office programs and avoid situations similar to those suffered by Mercer's counsel in its own practice.

The final portion of this article analyzes the duties of a lawyer who receives a file containing embedded data that reveals confidential or privileged information of an opposing party. Is that lawyer bound by the same obligations that apply when documents in a misaddressed envelope are received, or, conversely, is the lawyer free to use and review the embedded information?

The Purpose of Metadata

Software does not embed data into documents to cause disclosure of confidential information. While the type and amount of embedded data will vary based on the particular program used, the primary function of metadata is utilitarian: It is designed to help users revise, organize, and access electronically created files. Typical metadata includes, for example, information about the person who authored the document and the location

David Hricik is an associate professor at Mercer Law School who has written several books and more than a dozen articles. He can be reached at *hricik_d@mercer.edu*. **Chase Edward Scott** is a JD candidate at Mercer Law School hailing from Chattanooga, TN. Following graduation in 2009, he intends to practice intellectual property law. This article is based upon an earlier version of an article from the *Georgia Bar Journal*, Vol. 13, No. 5 (Feb. 2008). Used with permission.

(drive, folder) where the file was saved. In addition, a file can include metadata records of past revisions. As a result, one can examine changes that have been made to a file and compare them visually to any hand-written revisions to ensure that they have, in fact, been made. Thus, embedded data may serve useful and legitimate purposes.

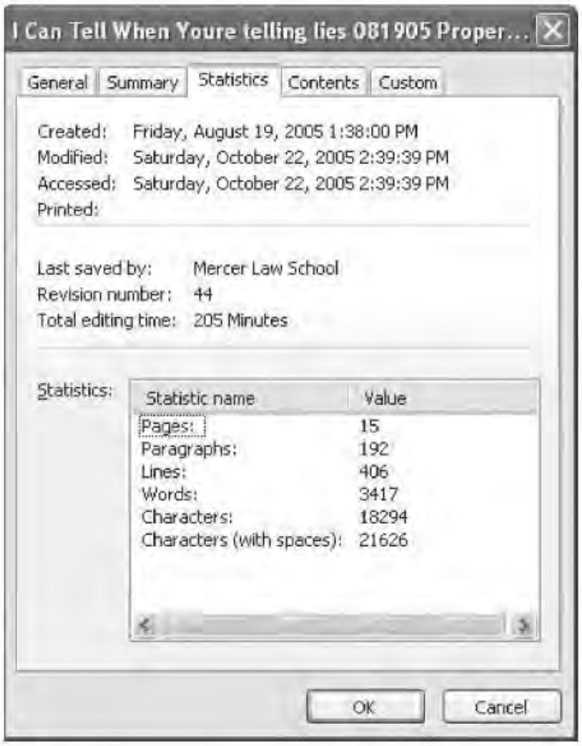
Metadata in Microsoft Word

Microsoft Word is a ubiquitous software program.[2] Lawyers everywhere commonly use it to create documents, and these files are regularly emailed in electronic form to clients, third parties, and opposing counsel. Unfortunately in some respects, embedded data is prevalent in Word, and the risk in electronically transferring sensitive metadata through Word files is substantial. The following illustrates embedded information typically found in Word documents:

File Properties Information

Basic metadata in a pre-2007 version of Word can be seen by reviewing the different menus available.[3] A key location is in the "Properties" subset menu, located within the "File" menu. The "Properties" for a particular document may reveal the author, creation dates, and other information. For example, an article by the authors contained the information shown in Figure 1:

Figure 1



Created: Friday, August 19, 2005 1:38:00 PM
Modified: Saturday, October 22, 2005 2:39:39 PM
Accessed: Saturday, October 22, 2005 2:39:39 PM
Printed:

Last saved by: Mercer Law School
Revision number: 44
Total editing time: 205 Minutes

Statistics:

Statistic name	Value
Pages:	15
Paragraphs:	192
Lines:	406
Words:	3417
Characters:	18294
Characters (with spaces):	21626

The metadata on that single screen alone reveals that the file was created in August and was still being worked on in October 2005. It also reveals that the document was in its 44th revision (meaning it had been opened and closed 44 times) and had been edited for a total of 205 minutes.[4] Had this document been work product for a client and had the author transmitted the file to the client in electronic form, the client would have been able to access this metadata to tell whether the lawyer had worked on the document for as long as indicated in the lawyer's fee statement. If it had been a report prepared by an expert witness sent to opposing counsel, the attorney could have discerned how long the expert had spent drafting the report. If it had been a brief prepared by an undisclosed attorney and forwarded to opposing counsel, the author's identity could have been revealed.[5] Metadata matters.[6]

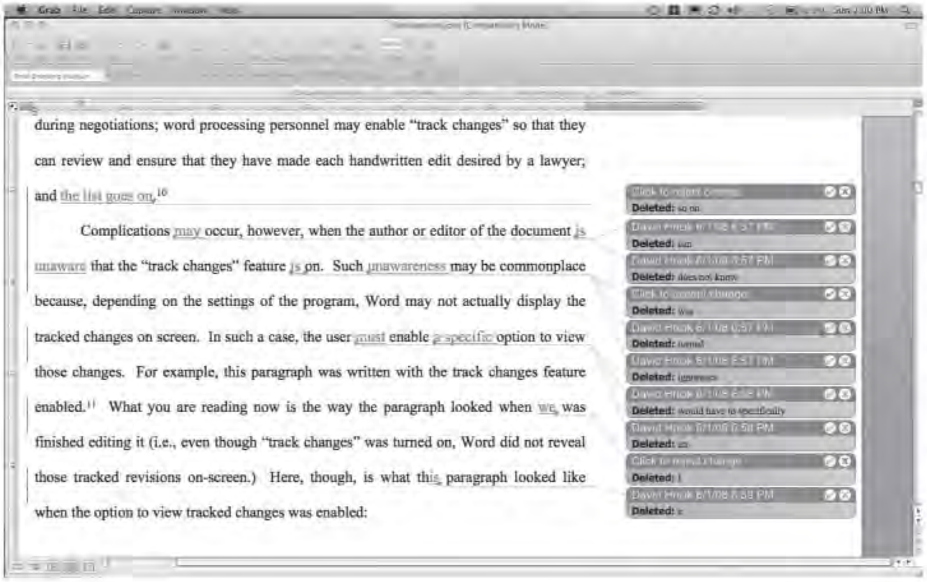
Track Changes Feature

More troubling than the basic metadata found in the File/Properties screen is the other unseen data that can accompany a Word file. Foremost, track changes is a feature within Word that creates a record of every change made to a document. It has many uses. Lawyers who exchange drafts of contracts, as mentioned in the introduction, can turn on this feature to allow prior revisions of a proposed contract to be reviewed during negotiations; word processing personnel may enable track changes so that they can review and ensure that they have made each handwritten edit desired by a lawyer; and the list goes on.[7]

Complications may occur, however, when the author or editor of the document is unaware that the track changes feature is on. Such unawareness may be commonplace because, depending on the settings of the program, Word may not actually display the tracked changes on screen. In such a case, the user must enable a specific option to view those changes. For example, this paragraph was written with the track changes feature enabled.[8] What you are reading now is the way that the paragraph looked when we were finished editing it (that is, even though track changes was turned on, Word did not reveal those tracked revisions on screen). Figure 2 (on page 24), though, is what this paragraph looked like when the option to view tracked changes was enabled.

Someone who received the file by email could easily reveal the changes and see the revisions shown above. If this document had been a contract instead of the current article, the metadata could have revealed to an opposing party the negotiator's mental process in working through revisions previously made to key proposed terms.[9] Such information could be valuable to the opposing party in formulating its strategy.

Figure 2



during negotiations; word processing personnel may enable "track changes" so that they can review and ensure that they have made each handwritten edit desired by a lawyer; and the list goes on.[10]

Complications may occur, however, when the author or editor of the document is unaware that the "track changes" feature is on. Such unawareness may be commonplace because, depending on the settings of the program, Word may not actually display the tracked changes on screen. In such a case, the user must enable a specific option to view those changes. For example, this paragraph was written with the track changes feature enabled.[11] What you are reading now is the way the paragraph looked when we was finished editing it (i.e., even though "track changes" was turned on, Word did not reveal those tracked revisions on-screen.) Here, though, is what this paragraph looked like when the option to view tracked changes was enabled:

Click to reject change
Deleted: so on

Deleted: can

Deleted: does not know

Click to accept change
Deleted: Was

Deleted: normal

Deleted: ignorance

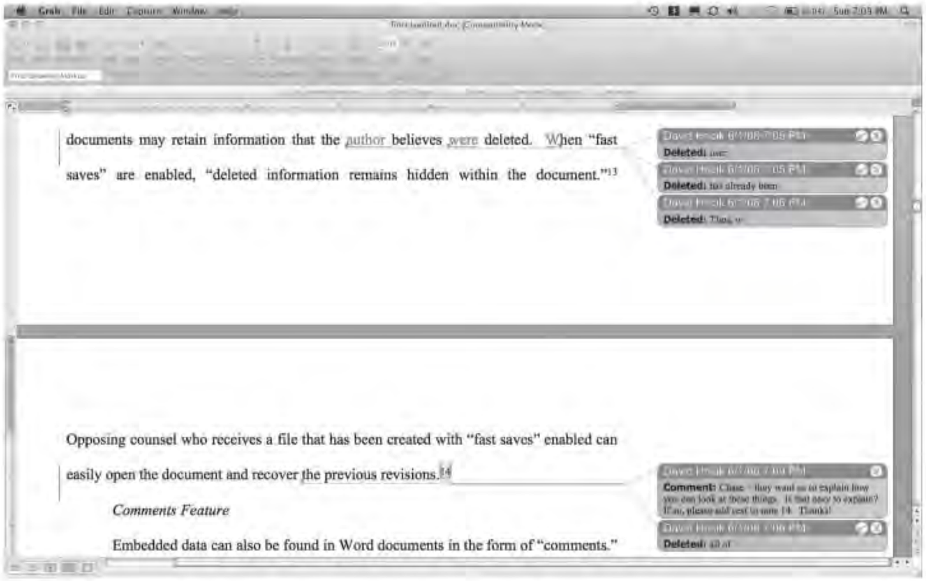
Deleted: would have to specifically

Deleted: as

Click to reject change
Deleted: I

Deleted: s

Figure 3



documents may retain information that the author believes were deleted. When "fast saves" are enabled, "deleted information remains hidden within the document."[13]

Deleted: has already been

Opposing counsel who receives a file that has been created with "fast saves" enabled can easily open the document and recover the previous revisions.[14]

Comments Feature

Embedded data can also be found in Word documents in the form of "comments."

Comment: Chase – they want us to explain how you can look at these things. Is that easy to explain? If so, please add text to note 14. Thanks!

Fast Saves Feature

Another form of embedded Word data is created by the use of "Fast Saves." This feature enables the user to quickly save the document without having to take the time to perform a full save; however, fast saves only append the changes to the end of the document file rather than replace the actual edited material. In other words, fast saved documents may retain information that the author believes were deleted. When fast saves are enabled, "deleted information remains hidden within the document."[10] Opposing counsel who receives a file that has been created with fast saves enabled can easily open the document and recover the previous revisions.[11]

Comments Feature

Embedded data can also be found in Word documents in the form of "comments." The comments feature is incredibly useful for collaboration. Comments are embedded within the file and accompany it when it is emailed. Figure 3 is a screen shot of a paragraph from the section above set to show tracked changes and comments.

Like track changes, the comments feature of Word can leave hidden data within an electronic document that may be valuable to opposing counsel.

Versions Feature

A final example of a type of hidden metadata in Word is created by the software's "versions" feature. If "versions" is enabled, each time that the file is saved, a new version is created and stored, leaving prior versions of the document intact.[12] Once again, if the file is transmitted to an opposing party, she could review every prior version of the document to see what changes had been made.[13]

The Duty to Avoid Disclosing Embedded Confidential Information

All of the listed features from Word are useful to lawyers or their word processing personnel. All need to be aware, however, that these tools embed hidden data within the file. Further, they need to recognize that their word processing staff may enable certain features without the lawyer's knowledge.[14] For example, if a lawyer is unaware that her secretary had enabled track changes and if the secretary failed to appreciate the problems created by transmitting the file with track changes still embedded, then it could cause a problem.

Risk of unintended disclosure has, of course, always existed, just in a different form. Not too long ago, the primary risk was that a letter intended for a client would instead be mailed to opposing counsel.[15] Similarly, a lawyer might have made handwritten comments on a contract proposal drafted by the other side, and, though intending to forward the document to the client for review, inadvertently mailed or faxed it to opposing counsel.

In the digital age, however, new methods for creating, editing, and transmitting documents have increased the risk of unintended disclosures. As discussed already, electronic files may now reveal more information than drafts from the past; they "can reveal a cache of information, including the names of everyone who has worked on . . . a specific document, text and comments that have been deleted, and different drafts of the document."[16] Because of the inherent dangers involved with transmitting metadata, it is important to discuss what professional duties lawyers owe their clients to safeguard this information.

To aid this discussion, we emphasize the distinction between *confidential* information, that which a lawyer has a professional duty to keep in confidence, and information that is *privileged*. The attorney-client privilege protects against forced disclosure of communications between lawyer and client.[17] The privilege is a qualified one, however, because only confidential communications *between the attorney and client* are protected. The privilege does not apply to information learned by the lawyer from third parties or even to the lawyer's conversations with the client conducted in the presence of others.[18]

While the attorney-client privilege protects against the forced disclosure of communications, lawyers themselves are restricted from disclosing confidential information unless authorized to do so by their client or by judicial authority. The confidential information covered by this duty is far broader than that covered by the attorney-client privilege, encompassing "all information relating to the representation, whatever its source . . . ."[19] Given this broad definition, there is a substantial risk that metadata transmitted by an attorney to a third party will contain confidential information. Accordingly, a lawyer who knows that a document contains embedded information generally has a duty to remove it before transmission.

But what about a lawyer who unknowingly transmits a document with embedded confidential information? Has that lawyer violated the duty of confidentiality? Some may argue that because "everyone knows" about metadata, any lawyer who fails to remove hidden confidential information has breached his or her professional duty.[20] In the authors' experience, though, the opposite is true: The vast majority of attorneys canvassed about this issue had never heard of metadata, let alone understood how to deal with it. In further support of this less-than-scientific observation, documents that contain embedded data have routinely shown up on the Web, some were even posted by large-firm lawyers who ostensibly should be the most educated about embedded data.

In any event, the existence of metadata and the dangers it presents for unintended disclosure are becoming more widely known and appreciated. Lawyers will soon, if the time has not already arrived, be unable to avoid negligence claims or defend against bar complaints by pleading ignorance of the risks that embedded information creates. Attorneys should make every effort to prevent transmission of confidential information. A few simple methods to aid in this effort are detailed in the following section.

How to Avoid Creating Embedded Data and How to Remove It

Several approaches addressing the prevention of inadvertent transmission of metadata are available. This section provides a brief summary of these methods.[21]

Avoid Creating Embedded Data

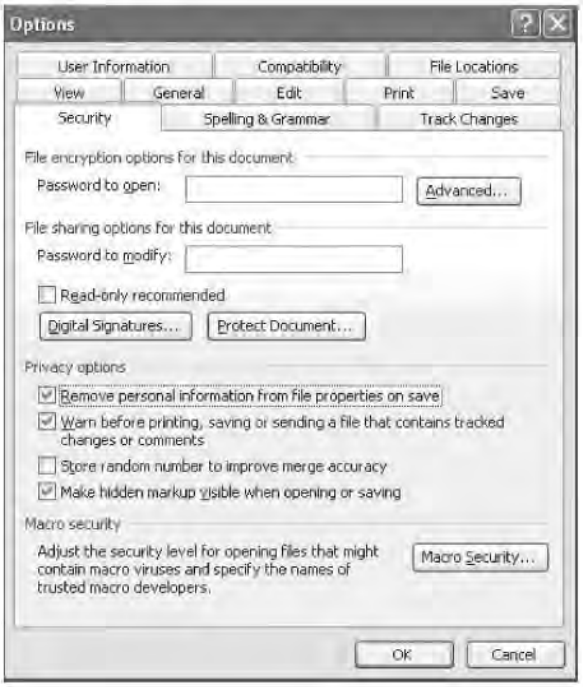
Obviously, the easiest way to avoid disclosure of embedded confidential information is not to create it in the first place. But, simply saving information to a hard drive or networked drive may retain information about the computer or network to which it is linked. To ensure that this location is not included in any file sent to a third party, attorneys should re-save each document to a floppy disk, the desktop, or to a flash drive using "Save As."

Beyond this simple tip, Microsoft and other developers have recognized the importance of maintaining the confidentiality of metadata in certain situations and have, in response, provided users with in-program options allowing them to alter the types and amount of embedded information that will be stored in their documents. The following describes simple measures lawyers can take to avoid creating or to limit the creation of embedded data when using some of the more commonly used office programs.

Microsoft Word 2003

Under the "Tools" menu, select "Options," and click on the "Security" tab. The resulting dialog box allows the user to encrypt the file, edit privacy options, and change the level of macro security. Checking the box "remove personal information from file properties on

Figure 4



File encryption options for this document

Password to open:

File sharing options for this document

Password to modify:

□ Read-only recommended

Privacy options

☑ Remove personal information from file properties on save

☑ Warn before printing, saving or sending a file that contains tracked changes or comments

□ Store random number to improve merge accuracy

☑ Make hidden markup visible when opening or saving

Macro security

Adjust the security level for opening files that might contain macro viruses and specify the names of trusted macro developers.

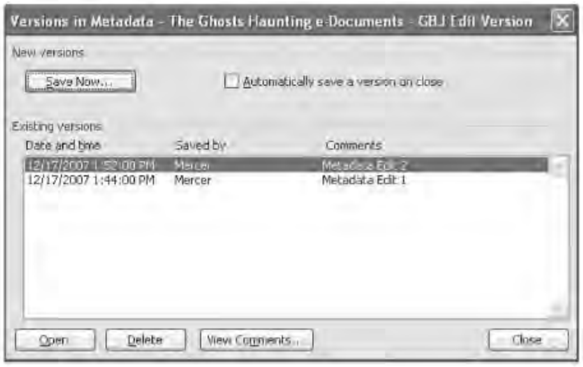
save" prevents the personal information associated with your computer, network, or registration information from attaching to the document. Thus, this option, shown in Figure 4, should be selected when the lawyer works on any potentially sensitive documents in Word that may be transmitted to outside parties.

Other information, such as the author of the document, contained in the "Summary" tab under "Properties" within the "File" menu, may also be considered sensitive and inappropriate for opposing counsel to view. The lawyer can remove any of the offending information from the document by simply deleting the entries in the text boxes and clicking "OK" to save revisions.[22]

As noted earlier, use of the fast saves feature of Word can leave hidden data in the document. To turn off fast saves, go to the "Tools" menu, select "Options," and click on the "Save" tab. Under the "Save" tab, ensure that the "allow fast saves" box is not selected.[23]

As also noted, Word allows users to save multiple versions of the same document, thus increasing the unintended disclosure of information contained in earlier versions. To determine whether any older versions of a file exist, go to the "File" menu and click on "Versions." Any old versions attached to the document will be listed by the date/time and creator of the saved version. To remove a version, simply click on the offending entry and select delete.[24] This is shown in Figure 5.

Figure 5


Versions in Metadata - The Ghosts Haunting e-Documents - GBJ Edit Version
Save Now...
Open
Delete
View Comments...
Close

New versions

□ Automatically save a version on close

Existing versions

Date and time	Saved by	Comments
12/17/2007 1:52:00 PM	Mercer	Metadata Edit 2
12/17/2007 1:44:00 PM	Mercer	Metadata Edit 1

Microsoft PowerPoint 2003

Similar to Word, Microsoft PowerPoint will track, via normally hidden metadata, personal information such as the identity of the author of the document. To remove this metadata from a PowerPoint file, go to the "Tools" menu and select "Options." Under the "Security" tab, ensure that "remove personal information from file properties on save" is checked.[25] To delete the user name and initials associated with the file, click on the "General" tab in this same submenu. From here, the user can simply highlight and delete the unwanted information.[26]

Finally, it is important to note that PowerPoint documents often contain embedded files from other programs that may, in turn, contain their own metadata. To ensure that the embedded objects are metadata free, right click the object to be embedded and select "cut." From there, select the desired slide, go to the "Edit" menu, and select "Paste Special."[27] This newly created image will be free from sensitive information concerning its source.

Microsoft Excel 2003

Many of the same processes used to eliminate metadata from Word and PowerPoint files can also be used to eliminate personal data from Microsoft Excel; however, Excel presents several unique methods for retrieving personal data that attorneys should be aware of prior to sending workbook files to opposing counsel. For instance, in Excel, users have the ability to hide individual rows, or columns of cells from view. To view these hidden cells, hit Ctrl+Shift+Space Bar to select all of the cells in the workbook, then go to the "Format" menu, and find the submenu for "Row." Under this submenu, select "Unhide." Repeat this process for the "Column" and "Sheet" submenus. This should make all hidden cells and sheets visible and capable of being deleted if the information contained therein is found to be confidential.[28]

Excel users can also link formulas between multiple workbooks (shown in Figure 6). Though a useful tool, these formulas may contain metadata concerning the documents to which they are linked. To remove this potentially sensitive data, highlight the linking formula, right click, and select "Copy;" following this, go to the "Edit" menu, and click "Paste Special;" select "Values" and click "OK." Note that this will result in the formula being deleted from the document; however, the resulting data will remain in the workbook.[29]

Figure 6

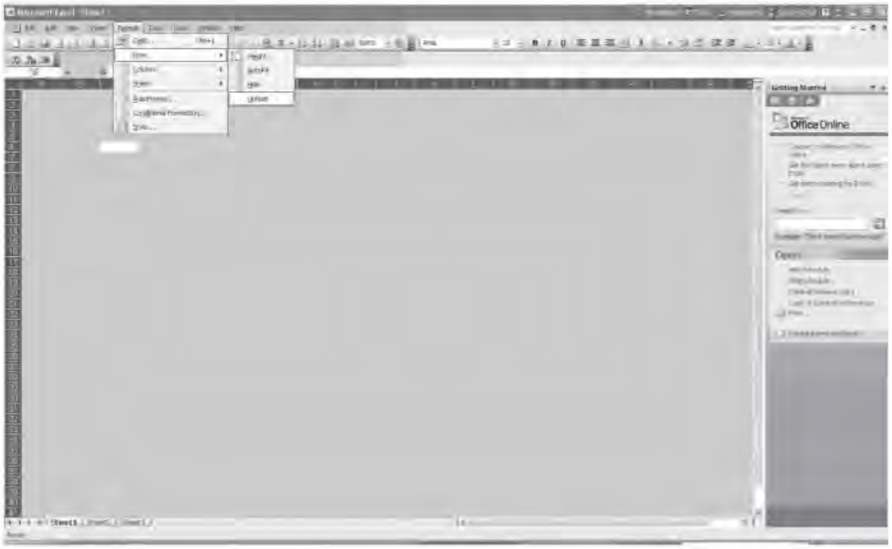
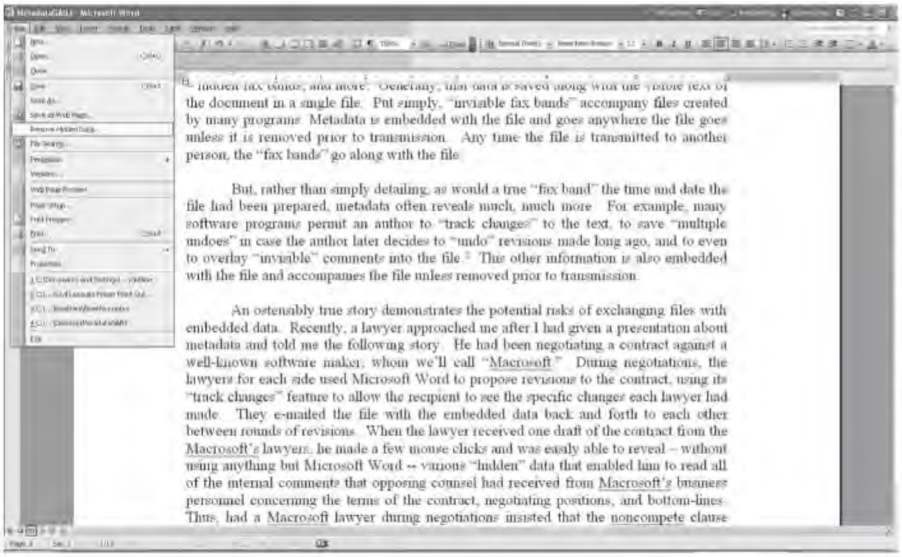


Figure 7



hidden fax bands, and more. Generally, that data is saved along with the visible text of the document in a single file. Put simply, "invisible fax bands" accompany files created by many programs. Metadata is embedded with the file and goes anywhere the file goes unless it is removed prior to transmission. Any time the file is transmitted to another person, the "fax bands" go along with the file.

But, rather than simply detailing, as would a true "fax band" the time and date the file had been prepared, metadata often reveals much, much more. For example, many software programs permit an author to "track changes" to the text, to save "multiple undoes" in case the author later decides to "undo" revisions made long ago, and to even to overlay "invisible" comments into the file.[2] This other information is also embedded with the file and accompanies the file unless removed prior to transmission.

An ostensibly true story demonstrates the potential risks of exchanging files with embedded data. Recently, a lawyer approached me after I had given a presentation about metadata and told me the following story. He had been negotiating a contract against a well-known software maker, whom we'll call "Macrosoft." During negotiations, the lawyers for each side used Microsoft Word to propose revisions to the contract, using its "track changes" feature to allow the recipient to see the specific changes each lawyer had made. They e-mailed the file with the embedded data back and forth to each other between rounds of revisions. When the lawyer received one draft of the contract from the Macrosoft's lawyers, he made a few mouse clicks and was easily able to reveal – without using anything but Microsoft Word -- various "hidden" data that enabled him to read all of the internal comments that opposing counsel had received from Macrosoft's business personnel concerning the terms of the contract, negotiating positions, and bottom-lines. Thus, had a Macrosoft lawyer during negotiations insisted that the noncompete clause

Removing Embedded Data before Transmitting

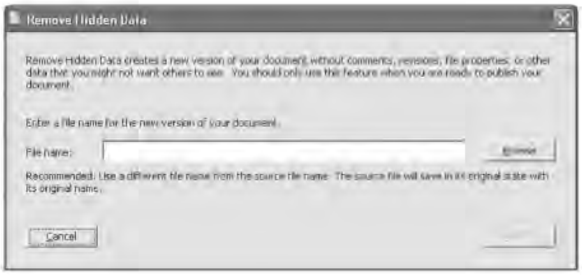
While these methods can help reduce the amount of metadata created and stored in electronic files, attorneys should also consider taking additional precautions to remove any other embedded information that has made its way into a file before transmission.[30] There are a number of methods to accomplish this task. Because reasonable care is necessary to satisfy the lawyer's duty of confidentiality, the nature of the communication at issue will indicate what steps are required for particular communications or practices.

Large software makers know about the problems that unintentional transmission of metadata can create for lawyers and have updated their programs with additional functionality to avoid creating, avoid transmitting, find and remove this embedded data. Microsoft created a free add-in, which can be downloaded from the company's Web site. It is designed to eliminate most sensitive information from documents created in Microsoft Office programs, even when the document was drafted with a metadata-creating feature turned on.[31] (Remember: Metadata has utility!) Many lawyers still use the pre-2007 version of the Microsoft Office Suite. Installation of this add-in will create an additional option to "Remove Hidden Data" within the "File" menu in your Microsoft Office programs shown in Figure 7.

After selecting this option, the user will be asked to enter a file name for what will become the "clean" version of the document. Once a name is provided, the user will click next to start the scan as shown in Figure 8 (on page 29).

When the scan is complete, a text file will open that contains a summary of the scanning results.[32] The end result is an effective, easy, and free solution to the problem of metadata transmission via Microsoft Office documents; you just have to remember to use it!

Figure 8



Remove Hidden Data

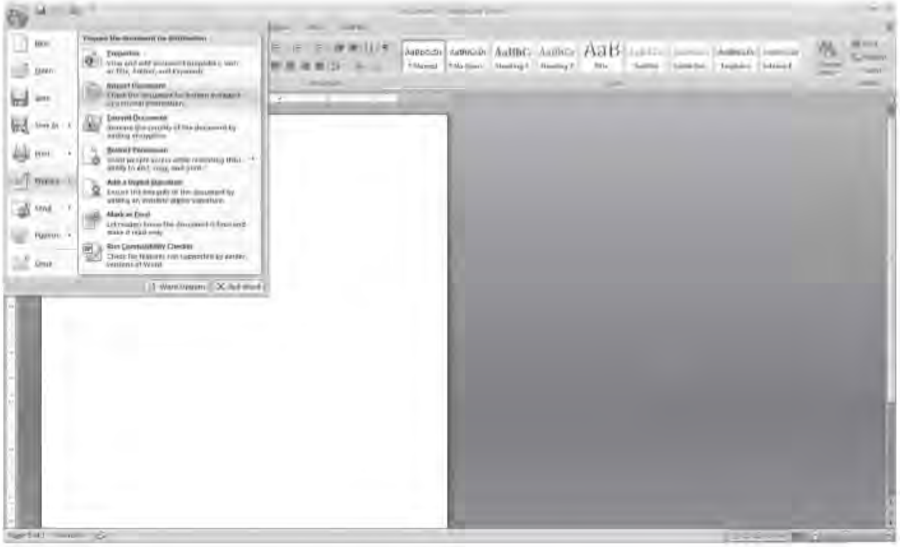
Remove Hidden Data creates a new version of your document without comments, versions, file properties, or other data that you might not want others to see. You should only use this feature when you are ready to publish your document.

Enter a file name for the new version of your document.

File name:

Recommended: Use a different file name from the source file name. The source file will save in its original state with its original name.

Figure 9



Saving a document in Portable Document Format (pdf) will also reduce the amount of metadata stored in the file. But this process does not eliminate metadata entirely.[33] For many purposes, simply saving a document in pdf format may suffice. Pdf files often cannot be easily modified, though, thereby reducing the efficiency and functionality of document exchanges.

Additionally, several commercial software scrubbers are available for purchase.[34] While these programs have differing degrees of functionality and integration with other software (such as Microsoft Outlook), they can all be used to scan files before they are transmitted and remove the embedded metadata.

Microsoft Office 2007

The newest edition of the Microsoft Office suite of applications has responded to user demand for metadata removal by including its own Document Inspector and removal tool in Microsoft Word, Excel, and Power Point 2007. Similar to the 2003 add-in, this Document Inspection tool is a quick and easy solution to the problem of metadata removal. To remove the unwanted information, first click on the Microsoft Office Button and select "prepare" from the drop down menu.[35] After highlighting "prepare," select "Inspect Document" from the menu that appears to the right (see Figure 9.)[36]

The document inspector window will open, at which point you will have the opportunity to deselect the types of metadata that you would like to avoid including in the metadata document search. After making this determination, press the "inspect" button (shown in Figure 10 on page 30.)[37]

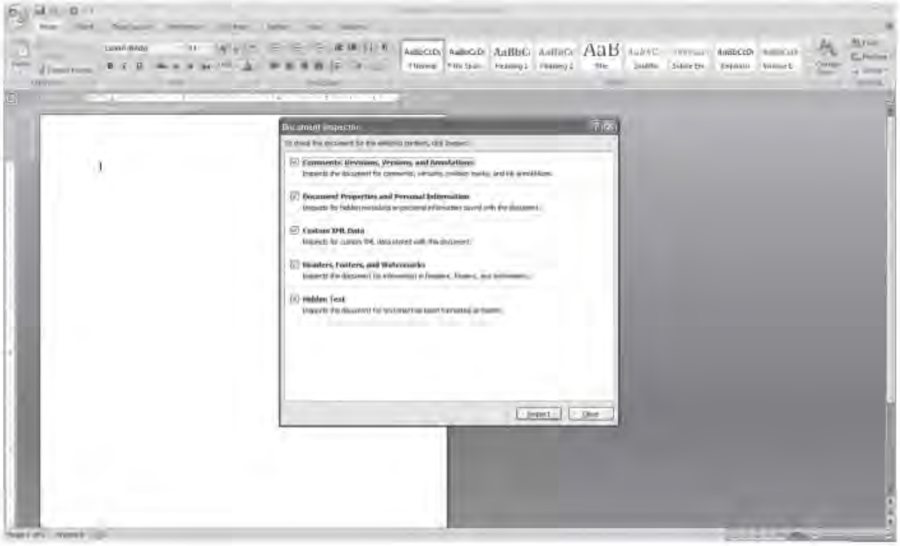
Following inspection, the window shown in Figure 11 (on page 30) will appear, revealing which categories of metadata are present in your document and giving you the opportunity to remove each category individually:

Categories of metadata that are present within the document will appear with a red exclamation mark to the left of the category description and a "remove all" button to the right. Simply press the "remove all" button to delete that category of metadata from the document. It is important to note that once metadata is removed in this manner or using the add-in tool for Microsoft Office 2007, it cannot be retrieved. Any important metadata that you do not wish to lose should be saved under a separate file name prior to its removal and kept for your own reference.[38]

Unintended Disclosure Agreements

A final, less technical way to avoid problems with embedded data is to have an agreement in place with opposing counsel by which the parties acknowledge beforehand that any transmission of confidential embedded data is unintentional and that any documents identified as containing such information should be deleted. Obviously, the efficacy of this option depends upon the trust of counsel, and when the mere viewing of the information would let the cat out of the bag, such agreements may be insufficient. In the final analysis, ensuring that embedded data is not created, or ensuring that it is stripped out before a file is sent, will normally be the only effective way to address the problems of embedded data.

Figure 10



Document Inspector

To check the document for the selected content, click Inspect.

☑ Comments, Revisions, Versions, and Annotations
Inspects the document for comments, versions, revision marks, and ink annotations.

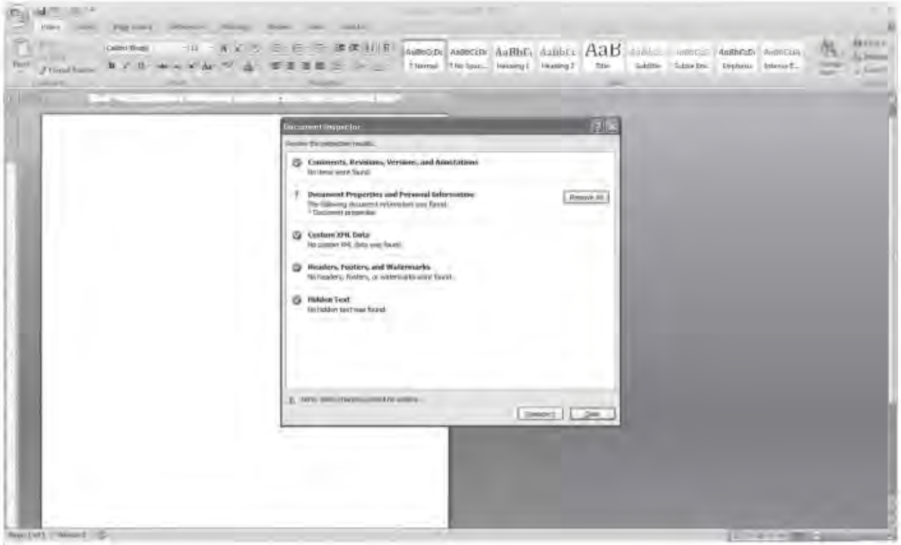
☑ Document Properties and Personal Information
Inspects for hidden metadata or personal information saved with the document.

☑ Custom XML Data
Inspects for custom XML data stored with this document.

☐ Headers, Footers, and Watermarks
Inspects the document for information in headers, footers, and watermarks.

☒ Hidden Text
Inspects the document for text that has been formatted as hidden.

Figure 11



Document Inspector

Review the inspection results.

Comments, Revisions, Versions, and Annotations
No items were found.

! Document Properties and Personal Information
The following document information was found:
* Document properties

Custom XML Data
No custom XML data was found.

Headers, Footers, and Watermarks
No headers, footers, or watermarks were found.

Hidden Text
No hidden text was found.

Note: Some changes cannot be undone.

Can You Look?

Given that metadata is a relatively new concern for lawyers, it is not surprising that formal ethical rules do not yet directly address the question of whether it is proper for a lawyer to search an electronic file sent by another lawyer to see if any useful embedded data is present. Most states have a general catchall rule, however, that prohibits "professional conduct involving dishonesty, fraud, deceit or misrepresentation."[39] Unfortunately, the bar associations that have analyzed the issue have openly split on whether it is ethical for a lawyer to look for metadata. The split is deep, direct, and irreconcilable.

On one end of the spectrum, the bars of New York, Florida, Arizona, and Alabama have concluded that conducting a purposeful search for metadata is unethical. The New York Bar Association emphasized that "it is a deliberate act by the receiving lawyer, not carelessness on the part of the sending lawyer, that would lead to the disclosure of client confidences and secrets" in the embedded data.[40] Alabama's Bar similarly condemned the act of mining for metadata as "a knowing and deliberate attempt by the recipient attorney to acquire confidential and privileged information in order to obtain an unfair advantage against an opposing party."[41] Florida's Bar also agreed but more softly wrote that a recipient should not try to view metadata that the lawyer knows or should know was not intended for his or her viewing.[42] Most recently, Arizona's Bar issued an opinion advising lawyers that as a general rule a lawyer may not "mine" documents from opposing counsel for metadata.[43]

On the other end of the spectrum, both the American Bar Association (ABA) and the Maryland Bar Association found nothing unethical with deliberately mining documents sent by opposing counsel outside the context of discovery for metadata.[44] The ABA expressed its disagreement in mild terms, however, stating only that "the Committee does not believe that a lawyer . . . would violate" his or her professional duties by mining for metadata.[45] Taking a slightly more nuanced approach, the District of Columbia Bar reasoned that viewing metadata was dishonest only if, before viewing it, the lawyer *actually knew* that the metadata had been inadvertently sent.[46] If the attorney was made aware of the inadvertent transmission of the information halfway through the initial review of the document, any further review of the confidential material would be seen as professional misconduct under the District of Columbia opinion.[47] Recently, the Colorado Bar was hesitant to go as far as the District of Columbia, instead holding that, without prior notice of the inadvertent transmission, a reviewing attorney is obligated only to notify the sending attorney of the inadvertent transmission, not to stop the review of the document entirely.[48]

Perhaps representing the more balanced view is a recent opinion from the Pennsylvania Bar Association. After noting the split, the Pennsylvania Bar refused to take a bright-line position on whether mining for metadata is unethical. Instead, it stated that "each attorney must determine for himself or herself whether to utilize the metadata contained in documents and other electronic files based upon the lawyer's judgment and the particular factual situation."[49] Similarly, the Pennsylvania Bar stated that whether the information should be used turned upon "the nature of the information received, how and from whom the information was received, attorney-client privilege and work-product rules, and common sense, reciprocity and professional courtesy."[50]

Many lawyers are thus left with neither controlling authority nor a clear majority rule from those authorities that have addressed the question of whether it is ethical to mine for metadata. If the opinions suggest anything, it is that a lawyer who decides to mine for embedded data should proceed with caution, particularly if the embedded data reveals either the other side's client confidences, privileged information, or work product and the circumstances are such that a reasonable lawyer would know that the embedded data was sent inadvertently. More fundamental than whether the lawyer will be disciplined for examining embedded data is the question of whether it is professional to do so. The ethics rules decide only matters of discipline, and the broader and greater question of whether it is "right" to look should not be lost. Not only does the adage of "what goes around comes around" apply, but a judge may question the integrity of a lawyer who intentionally takes advantage of an opponent's mistake that reveals privileged information, for example. More is at stake than discipline.

Assuming, however, that a lawyer comes across metadata in an exchanged document either by intentionally mining for it or through innocent discovery, does the lawyer have any obligation to notify the sender of the existence of the metadata?

Must the Recipient Notify the Sender of the Mistake?

A lawyer may learn of the existence of embedded data intentionally—the issue discussed above—or by mistake. As shown, a lawyer can actively mine for metadata contained within a document. At the same time, an attorney who creates a document with track changes turned on may believe that the record of changes is free from the unintended viewer's prying eyes so long as the track changes setting has been changed from "Final Showing Markup" to "Final."[51] Without the proper removal of metadata, any holder of the electronic document maintains the ability to manipulate that document in the same manner as the document's creator. This means that, when a lawyer opens a document sent from opposing counsel and currently has track changes set to "Final Showing Markup," that document will show all track changes regardless of the original creator's track changes setting. If sensitive information had previously been deleted from the document by its creator, the unwitting attorney could inadvertently be exposed to this information and may be faced with a serious ethical obligation. While most metadata is discovered through intentional mining, accidental exposure to embedded data is still possible.[52]

Many states expressly impose an obligation upon a lawyer who is inadvertently sent a document to notify opposing counsel of the mistake. Specifically, Model Rule of Professional Conduct 4.4(b) requires a "lawyer who receives a document relating to the representation of the lawyer's client . . . [who] knows or reasonably should know that the document was inadvertently sent" to "promptly notify the sender."[53] The comments also specifically state that the rule covers inadvertently sent email.[54] Model Rule 4.4(b), however, has only been adopted in a few jurisdictions.[55]

In the context of misdirected faxes, mail, email, and other communications besides embedded data, the authorities have generally recognized that ethical obligations can arise when a lawyer receives a document that was not intended for him or her,[56] such as the receipt of a fax intended for opposing counsel's client.[57] As a general principle, those authorities hold that, when a lawyer receives privileged or confidential client information from another lawyer and when the circumstances reasonably show that the disclosure was inadvertent, the recipient must notify the sender of the mistake and, in some jurisdictions, follow the sender's instructions on how to proceed next.[58]

Assuming that such a duty exists in your jurisdiction, the question would be whether that duty should apply in the special context of embedded data. Several bar associations have analyzed this duty in the context of embedded data when the lawyer intended to send the file containing that data to the lawyer who received the file but did not intend to transmit embedded confidential information. Unfortunately, those authorities have also split widely on whether the recipient has any duty to notify the sender of the presence of embedded data.

The opinions split along the same lines, essentially, as they do concerning whether it is dishonest to look.

Specifically, the ABA[59] and the Maryland Bar[60] concluded that there was no obligation to notify the sender, while Florida,[61] New York,[62] Arizona,[63] and Alabama[64] concluded that such an obligation exists. The District of Columbia concluded that an obligation to notify existed only if the lawyer had actual knowledge that the embedded data was sent inadvertently before examining it,[65] while Pennsylvania again adopted a facts-and-circumstances approach to the question.[66]

What, then, must a lawyer operating outside of these jurisdictions do when faced with this situation? Without clear guidance, the best advice would be the same as that regarding how to handle whether mining is appropriate; the greater the significance of the information and the clearer it is that the information was sent by mistake, the more likely it is that it is unethical not to notify the sender of the presence of embedded data. Whether inadvertent transmission waives the attorney-client privilege is, of course, a different question, and how the lawyer should proceed after notification—whether he should follow the sender's, his client's, or his own view of what to do—is itself a complex issue unaddressed by many authorities.

Conclusion

Many lawyers are, at least for the time being, at an impasse when it comes to the treatment of opposing counsel's metadata. As the significance of metadata becomes more widely known, each state will no doubt develop its own approach to the treatment of inadvertent disclosure of confidential information through metadata. Until such a time arrives in every jurisdiction, we hope that, at a minimum, we have provided a warning as to where these problems await and some guidance regarding how to emerge from this ethical predicament unscathed.

Notes

1. Definition of Metadata, *http://wordnet.princeton.edu/perl/webwn?s=metadata* (last visited Dec. 4, 2007).
2. Andrew Beckerman-Rodau, "Ethical Risks from the Use of Technology," 31 *Rutgers Computer & Tech. L.J.* 1, 32 (2004); Brian D. Zall, "Metadata: Hidden Information in Microsoft Word Documents and Its Ethical Implications," 33 *Colo. Law.* 53, 53 (Oct. 2004) (describing legal profession's widespread adoption of Microsoft Word).
3. Interestingly, most metadata is stored in the last blank space of a Word document. If, for example, you select all of a Word document except its last space (which will appear to be blank), and then copy and paste that material into a new Word document, most metadata will not follow along. For a more technical discussion of how metadata is embedded in a Word document, *see* Zall, 33 *Colo. Law.* at 54.
4. To be clear, the file could simply have been open on the screen for 205 minutes. Thus, the amount of time indicated does not necessarily mean that the file was being worked on for all of those 205 minutes.
5. The kind and amount of information stored in the "Properties" file can be customized. To see whether your version has been customized, click on the "Custom" tab at the top of the "Properties" dialog box.
6. There are a number of other sources of metadata. For example, other tabs in the "Properties" dialog box depicted show where the file was stored on the author's hard drive and other information.
7. *See generally* James Veach, "Commutation Agreements: Drafting a Clear and Comprehensive Contract," 854 *PLI/Comm* 43 (2003) (noting that track changes can be used to aid in the drafting process).
8. To turn on "track changes," go to the "Tools" menu and to "track changes." To see whether an open document contains tracked changes, turn on track changes and then ensure that you have selected the "final showing markup" on the "Review" toolbar that appears.
9. *See* Zall, 33 *Colo. Law.* at 55-56 (collecting hypotheticals on how metadata could harm clients and lawyers when transmitted to opposing counsel).
10. Toby Brown, "Special Handling: How Paper and Electronic Files Differ," 21 *GPSolo* 22, 23 (Sept. 2004). This is done by selecting "Save As" from the "File" menu, then selecting "Tools," and then "Save Options." One option is "Allow Fast Saves." Fast saves is "very useful in the event of hardware failure because it reduces the chance of losing changes to a document." *Id.*
11. Documents that contain sensitive information should have fast saves disabled to prevent inadvertent disclosure. If fast saves are enabled, the illogical order of the saved information may result in a failure to completely delete the confidential information despite your best efforts to do so. Opening the Word document in a text editor (such as Windows Notepad) will typically reveal the previously "deleted" text. *http://support.microsoft.com/kb/287081/EN-US/*.
12. To view the previous versions attached to a document in Microsoft Word, simply click on "File" and select "Versions" from the drop down menu.
13. *See* Zall, 33 *Colo. Law.* at 54-55.
14. Florida Rule of Professional Conduct 4-5.3(b)(2) requires lawyers with direct supervisory authority over a non-lawyer to "make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer[.]"
15. *See generally* Am. B. Ass'n. Formal Eth. Op. 92-368 (1992) (describing such scenarios).
16. Jason Krause, "Hidden Agendas," 90 *Am. B. Ass'n. J.* 26 (July 2004).
17. *See* Bryant v. State, 651 S.E.2d 718, 725 (Ga. 2007).
18. *Id.*
19. Comment to Florida Rule of Professional Conduct 4-1.6.

20. For example, Vincent Polley, then-chair of the ABA's Cyberspace Law Committee has been quoted as saying that lawyers can no longer "plead ignorance when it comes to this stuff any more." Krause, 90 *Am. B. Ass'n. J.* at 26.

21. *See generally* Carole Levitt & Mark Rosch, "Making Metadata Control Part of a Firm's Risk Management," 28 *L.A. Law.* 40, 40 (Mar. 2005) (describing various means to remove metadata, including some of those discussed here); Storm Evans, "How to Commit Malpractice With a Computer," 29 *Law Pract. Mgmt.* 56 (Mar. 2003) ("If you must e-mail or otherwise deliver a Word document, consider using macros or a utility program to strip away the metadata").

22. How to Minimize Metadata in Word 2003, *http://support.microsoft.com/kb/825576/* (last visited Dec. 11, 2007).

23. For more information on "Fast Saves," visit Frequently Asked Questions About "Allow Fast Saves," *http://support.microsoft.com/kb/291181/*.

24. *http://support.microsoft.com/kb/825576/*.

25. How to Minimize the Amount of Metadata in Powerpoint 2002 Presentations *http://support.microsoft.com/default.aspx?scid=kb;EN-US;314800* (last visited Dec. 12, 2007).

26. *Id.*

27. *Id.*

28. How to Minimize Metadata in Microsoft Excel Workbooks, *http://support.microsoft.com/default.aspx?scid=kb;EN-US;223789* (last visited Dec. 12, 2007).

29. *Id.*

30. *See* Beckerman-Rodau, 31 at 32-33 (2004) (suggesting that lawyers should consider removing metadata); Gerald J. Hoenig, "Technology Property," 18 *Probate & Prop.* 51 (Sept. 2004) (same).

31. To download this add-in, visit *http://www.microsoft.com/downloads/details.aspx?FamilyId=144E54ED-D43E-42CA-BC7B-5446D34E5360&displaylang=en* or search for "remove hidden data" on *http://www.microsoft.com/downloads.*

32. Control Metadata in Your Legal Documents, *http://office.microsoft.com/en-us/help/HA011400341033.aspx* (last visited Dec. 12, 2007).

33. *See* Jason Krause, "Guarding the Cyberfort," 39 *Ark. Law.* 24, 31 (2004). Suggestions, however, that pdf files contain *no* metadata are incorrect. *See, e.g.*, Hoenig, 18 *Probate & Prop.* 51; 1 Ronald E. Mallen & Jefrey M. Smith Legal Malpractice § 2.26 (2005) (stating that conversion from Word to pdf "could eliminate meta-data information"). Most pdf files do contain some metadata; thus, converting a Word file to a pdf file will simply result in *different* metadata being transmitted.

34. Numerous "scrubbers" can be found through Google, simply searching for "metadata" and scrubber.

35. *http://office.microsoft.com/en-us/help/HA100375931033.aspx.*

36. *Id.*

37. *Id.*

38. *Id.*

39. Ga. R. Prof. Conduct 8.4(a)(4).

40. N.Y. St. B. Ass'n. Op. 749 (Dec. 14, 2001). All online ethics opinions and rules are available through *http://www.hricik.com/StateEthics.html.*

41. Ala. Op. 2007-02 (March 14, 2007) ("it is ethically impermissible for an attorney to mine metadata from an electronic document he or she receives inadvertently or improperly from another party.").

42. Florida Prof. Eth. Comm. Op. 06-2 (Sept. 15, 2006).

43. St. B. Ariz. Op. 07-03 (Nov. 2007).

44. Am. B. Ass'n. Formal Opinion 06-442 (Aug. 5, 2006). *See* Md. B. Ass'n. Eth. Op. 2007-9 (2007) (not unethical to view metadata).

45. ABA Op. 06-442 at 4 n.10. The ABA also stated that it "views similarly" the Florida Bar Association's conclusion that mining metadata was unethical. *Id.*

46. D.C. B. Eth. Op. 341 (2007).

47. *Id.*

48. Co. Eth. Op. 119 (2008).

49. Pa. Formal Eth. Op. 2007-500 (Jan. 2008).

50. *Id.*

51. As discussed in our previous article, views may be changed in Microsoft Word to allow the user to either see or not see changes that have been made to a document. Thus, it is possible that a lawyer may, depending on the view she has set in Word, not even know she is transmitting embedded data in an exchanged document.

52. We created a copy of this file with track changes on, but the "Show" toolbar for track changes showing "Final," and then saved the file and emailed it. When the recipient opened the file with his "Show" toolbar set to "Final Showing Markup," all of the changes were visible. Thus, it is possible for a recipient to unintentionally view metadata. The discussion in this section, however, would likely apply whether the lawyer learned of the presence of embedded data intentionally, or by mistake.

53. Model Rules Of Prof'l Conduct R. 4.4(b).

54. *Id.*

55. Andrew M. Perlman, "Untangling Ethics Theory from Attorney Conduct Rules: The Case of Inadvertent Disclosures," 13 *Geo. Mason L. Rev.* 767, 783-785 (2006) (listing jurisdictions that had adopted Model Rule 4.4(b)).

56. The ABA mentioned inadvertent transmission of email when analyzing waiver of privilege over a misdirected fax: "the availability of xerography and proliferation of facsimile machines and electronic mail make it technologically ever more likely that through inadvertence, privileged or confidential materials will be produced to opposing counsel by no more than the pushing of the wrong speed dial number on a facsimile machine." ABA Formal Op. 92-368 (Nov. 10, 1992). *Accord* Fla. St. Bar Assn. Comm. On Prof. Ethics Op. 93-3 (Feb. 1, 1994) ("Such an inadvertent disclosure might occur as part of a document production, a misdirected facsimile or electronic mail transmission, a 'switched envelope' mailing, or misunderstood distribution list instructions.").

57. ABA Formal Op. 92-368 (Nov. 10, 1992). *Accord* Fla. St. Bar. Assn. Comm. on Prof. Ethics Op. 93-3 (Feb. 1, 1994) ("Such an advertent disclosure might occur as part of a document production, a misdirected facsimile or electronic mail transmission, a 'switched envelope' mailing, or misunderstood distribution list instructions.").

58. *See generally* Douglas R. Richmond, "Key Issues in the Inadvertent Release and Receipt of Confidential Information," 72 *Def. Couns. J.* 110 (2005); James Q. Walker, "Ethics and Electronic Media," 716 *PLI/Lit* 313, 334-336 (2004).

59. Am. B. Ass'n. Formal Op. 06-442, *supra*, n.44.

60. Md. B. Ass'n. Eth. Op. 2007-9. *supra,* n.44.

61. Florida Prof. Eth. Comm. Op. 06-2, *supra*, n.42.

62. N.Y. St. B. Ass'n. Op. 749, *supra,* n.40.

63. Ariz. Op. 07-03, *supra*, n.43.

64. Ala. Op. 2007-02, *supra*, n.41.

65. D.C. B. Eth. Op. 341, *supra,* n.46.

66. Pa. Formal Eth. Op. 2007-500, *supra,* n.49.

Exhibit J

GIBSON, DUNN & CRUTCHER LLP
Randy M. Mastro
Alexander H. Southwell (*pro hac application pending*)
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.3825
Fax: 212.351.5219
E-mail: RMastro@gibsondunn.com
Attorneys for Nonparty Gibson, Dunn & Crutcher LLP

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA v. WILLIAM BARONI, et. al, Defendants.	No. 2:15-cr-00193-SDW

OBJECTIONS AND RESPONSES OF NONPARTY GIBSON, DUNN & CRUTCHER LLP TO ORDER ON DEFENDANTS' APPLICATION FOR SUBPOENA *DUCES TECUM*

Pursuant to Rule 17 of the Federal Rules of Criminal Procedure, Nonparty Gibson, Dunn & Crutcher LLP ("GDC" or the "Firm") hereby objects and responds to the Order issued on July 10, 2015, on the application of Defendants Bridget Anne Kelly ("Kelly") and William E. Baroni, Jr. ("Baroni") (collectively, "Defendants"), for a subpoena *duces tecum*. GDC's objections as set forth herein are made without prejudice to GDC's right to assert any additional or supplemental objections pursuant to Rule 17 and other authorities.

GENERAL OBJECTIONS

GDC makes the following general responses and objections ("General Objections") to each item listed in Defendants' Subpoena *Duces Tecum* ("Items"). These General Objections are hereby incorporated into each specific response. The assertion of the same, similar, or additional objections or partial responses to individual Items does not waive any of GDC's General Objections.

1. GDC provides these objections and responses to the best of its current knowledge. GDC's response to any particular Item should not be taken as an admission that it accepts or admits the existence of any fact set forth or assumed by the Item, or that the response constitutes admissible evidence. No response to any portion of any Item shall be deemed a waiver of any objection not set forth herein that could be made to any such portion of the Item regarding relevancy of the information or its admissibility. Rather, these responses and any information or documents produced reflect GDC's attempt to produce non-privileged information and documents as they are kept in the ordinary course of business and within the timeline set forth by the Court and applicable law.

2. GDC objects to each and every Item to the extent it seeks to impose upon the Firm any obligations broader than, different from, or in addition to those imposed by the Federal Rules of Criminal Procedure, the Federal Rules of Evidence, the Local Rules of the United States District Court for the District of New Jersey, or the Court's Orders.

3. GDC objects to each and every Item to the extent it seeks to elicit a response that would require GDC to draw a legal conclusion or implicate the mental impressions of counsel in order to make a proper response.

4. GDC objects to each and every Item to the extent it seeks information that is protected from disclosure by the attorney-client privilege, the attorney work product doctrine, or any other applicable privilege, doctrine, or immunity. The inadvertent production by GDC of information protected from disclosure by any such privilege, doctrine, or immunity shall not be deemed a waiver by GDC of such privileges or protections.

5. GDC objects to each and every Item to the extent it seeks irrelevant information about GDC's operations. Such requests are overbroad and unduly burdensome. GDC will produce only information that is relevant to the Counts of the Indictment against Defendants.

6. GDC objects to each and every Item to the extent it would impose a duty on GDC to undertake a search for or an evaluation of information, documents, or things for which Defendants are equally able to search for and evaluate. In particular, GDC objects to each Item to the extent it seeks information or documents that are publicly available or readily available to Defendants. GDC further objects to each Item to the extent it seeks information that can be derived or ascertained from documents that will be produced in discovery by the prosecution or that are uniquely in the possession, custody, and control of Defendants.

7. GDC objects to the Items to the extent they purport to require GDC to identify or describe "any," "all," or other similarly expansive, infinite, or all-inclusive terms thereby rendering such Items unreasonable and oppressive, Fed. R. Crim. P. 17(c)(2), because they are overbroad and unduly burdensome.

8. GDC objects to the Items to the extent they seek information that is not in the possession, custody, or control of GDC, or purport to require GDC to speculate about the identity of persons who might have responsive documents.

9. GDC objects to the Items to the extent they are not limited in time and seek information for periods of time that are not relevant to any Count of the Indictment against Defendants.

10. GDC responds to each and every Item without waiving, or intending to waive, but to the contrary, preserving and intending to preserve: (a) the right to object to the use of any information or documents for any purpose in whole or in part, in any subsequent proceeding in

this litigation or in any other action on the grounds of competency, privilege, relevance or materiality, and (b) the right at any time to revise or clarify any of the responses made herein.

11. GDC will make, and has made, reasonable efforts to respond to Defendants' Subpoena *Duces Tecum*, to the extent that no objection is made, as GDC reasonably understands and interprets each Item. By responding to these Items, GDC does not concede the relevance or materiality of any of the Items or of the subjects to which they refer. GDC's responses are made subject to and without waiving any objections as to the competency, relevancy, materiality, privilege, or admissibility of any of the responses, or of the subject matter to which they concern, in any proceeding in this action or in any other proceeding. If Defendants subsequently assert any interpretation of any Item that differs from the interpretation of GDC, then GDC reserves the right to supplement and amend its objections and responses.

OBJECTIONS AND RESPONSES TO ITEMS

Subject to the foregoing qualifications and General Objections, as well as the specific objections made below, GDC objects and responds to Defendants' Subpoena *Duces Tecum* as follows:

ITEM NO. 1

Any and all handwritten or typed notes, stenographic transcripts and audio and/or video recordings of witness interviews conducted by Gibson Dunn during its representation of the Office of the Governor of New Jersey from on or about January 16, 2014 to the present.

RESPONSE TO ITEM NO. 1

GDC objects to this Item as unreasonable and oppressive; overly broad, unduly burdensome, vague, ambiguous; and as not authorized by Fed. R. Crim. P. 17(c)(2). GDC further objects to this Item to the extent it seeks information protected from disclosure by the attorney-client privilege, the attorney work product doctrine, or any other applicable privilege, doctrine, or immunity.

Subject to the foregoing General and Specific Objections, GDC responds as follows:

No documents exist responsive to this Item other than the 75 interview memoranda publicly released on April 14, 2014. GDC is today furnishing Defendants, through counsel, with the 75 interview memoranda.

ITEM NO. 2

Any and all metadata and the document properties for all typed notes and interview summaries created during interviews of witnesses during Gibson Dunn's representation of the Office of the Governor of New Jersey from on or about January 16, 2014 to the present.

RESPONSE TO ITEM NO. 2

GDC objects to this Item for all of the grounds set forth in the Motion of Nonparty Gibson, Dunn & Crutcher LLP to Quash Subpoena *Duces Tecum*, including because the Item is unreasonable and oppressive; overly broad, unduly burdensome, vague, ambiguous; and as not authorized by Fed. R. Crim. P. 17(c)(2). GDC further objects to this Item to the extent it seeks information protected from disclosure by the attorney-client privilege, the attorney work product doctrine, or any other applicable privilege, doctrine, or immunity.

DATE: August 21, 2015

GIBSON, DUNN & CRUTCHER LLP

By: s/ Randy M. Mastro
Randy M. Mastro
Alexander H. Southwell (*pro hac application pending*)
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.3824
Fax: 212.351.5219
E-mail: RMastro@gibsondunn.com
Attorneys for Nonparty Gibson, Dunn & Crutcher LLP